



Guide de l'utilisateur

Amazon Elastic Compute Cloud



Amazon Elastic Compute Cloud: Guide de l'utilisateur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon sont la propriété de leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Présentation d'Amazon EC2	1
Fonctionnalités	1
Services connexes	2
Accéder à EC2	4
Tarification	5
Estimations, facturation et optimisation des coûts	6
Ressources	7
Didacticiel de premiers pas	8
Étape 1 : Lancer une instance	10
Étape 2 : Connexion à l'instance	11
Étape 3 : Nettoyage de votre instance	15
Étapes suivantes	15
Bonnes pratiques	17
Amazon Machine Images	20
Utiliser une AMI	21
Créer votre propre AMI	21
Acheter, partager et vendre des AMI	22
Annuler l'enregistrement de votre AMI	22
Amazon Linux 2023 et Amazon Linux 2	23
AMI Windows	23
Types d'AMI	24
Autorisations de lancement	24
Stockage pour le périphérique racine	25
Types de virtualisation	30
Modes de démarrage	34
Lancer une instance	35
Paramètre de mode de démarrage AMI	43
Mode de démarrage du type d'instance	45
Mode de démarrage de l'instance	46
Mode de démarrage du système d'exploitation	49
Définir le mode de démarrage AMI	51
Variables UEFI	56
UEFI Secure Boot	57
Rechercher une AMI	72

Trouvez une AMI à l'aide de la console Amazon EC2	73
Trouvez une AMI à l'aide du AWS CLI	75
Trouvez une AMI à l'aide du AWS Tools for Windows PowerShell	75
Rechercher une AMI à l'aide d'un paramètre de Systems Manager	76
Trouvez les dernières AMI à l'aide de Systems Manager	81
Plus d'informations sur la recherche d'AMI	82
AMI partagées	82
Fournisseur vérifié	83
Rechercher des AMI partagées	84
Rendre une AMI publique	88
Partager une AMI avec des organisations ou des unités d'organisations	98
Partager une AMI avec des comptes AWS spécifiques	109
Annulation du partage d'une AMI avec votre compte	114
Utiliser des signets	116
Consignes pour les AMI Linux partagées	117
AMI payantes	123
Vendre votre AMI	125
Rechercher une AMI payante	125
Acheter une AMI payante	127
Obtenir le code produit pour votre instance	127
Utiliser le support payant	128
Factures pour les AMI payantes et supportées	129
Gérez vos AWS Marketplace abonnements	129
Cycle de vie de l'AMI	130
Créer une AMI	131
Modification d'une AMI	205
Copier une AMI	206
Stockage et restauration d'une AMI	217
Rendre obsolète une AMI	228
Désactiver une AMI	236
Archiver des instantanés d'AMI	242
Désenregistrer (supprimer) une AMI	242
Automatiser le cycle de vie des AMI basées sur EBS	252
Chiffrement AMI	252
Scénarios de lancement d'instances	253
Scénarios de copie d'images	257

Surveiller des événements d'AMI	259
Événements AMI	260
Créer des EventBridge règles Amazon	263
Comprendre la facturation d'AMI	267
Champs de facturation d'AMI	267
Rechercher les informations de facturation d'AMI	270
Vérifier les frais d'AMI sur votre facture	272
Quotas d'AMI	273
Demande d'une augmentation de quota pour les AMI	274
instances	276
instances et AMI	276
instances	277
AMI	280
Types d'instances	281
Types d'instance disponibles	282
Spécifications matérielles	283
Types de virtualisation AMI	285
Rechercher un type d'instance	286
Obtenir des recommandations	288
Modifier le type d'instance	296
Instance de performance à capacité extensible	308
instances GPU	365
instances Mac	376
Considérations	378
Préparation de l'instance	379
AMI macOS EC2	380
EC2 macOS Init	380
Moniteur système Amazon EC2 pour macOS	380
Ressources connexes	381
Lancer une instance Mac	381
Connexion à votre instance Mac	384
Mettre à jour le système d'exploitation et le logiciel sur les instances Mac	387
Augmenter la taille d'un volume EBS sur votre instance Mac	395
Arrêt ou résiliation de votre instance Mac	396
Trouvez les versions de macOS compatibles pour Dedicated Host	397
S'abonner aux notifications d'image AMI macOS	399

Notes de mise à jour des AMI EC2 macOS	400
Optimisation EBS	403
Types d'instance pris en charge	404
Obtenir les performances maximales	475
Afficher les types d'instances qui prennent en charge l'optimisation EBS	476
Activer l'optimisation EBS au lancement	478
Activer l'optimisation EBS pour une instance existante	479
Options d'achat d'instance	480
Déterminer le cycle de vie de l'instance	481
On-Demand instances	482
Reserved instances	485
Spot instances	560
Hôtes dédiés	668
Dedicated instances	732
Réserve de capacité	742
Cycle de vie d'une instance	832
Lancement d'une instance	834
Arrêt et démarrage de l'instance	834
Hibernation des instances	835
Redémarrage d'instance	836
Terminaison d'instance	836
Différences entre redémarrage, arrêt, mise en veille prolongée et résiliation	837
Lancer	839
Arrêt et démarrage	927
Mise en veille prolongée	936
Redémarrer	969
Terminer	971
Mise hors service	982
Résilience de l'instance	987
Utiliser des métadonnées d'instance	997
Utiliser IMDSv2	999
Configurer les options de métadonnées d'instance	1009
Récupérer des métadonnées d'instance	1035
Utiliser les données utilisateur d'instance	1059
Récupérer des données dynamiques	1063
Catégories de métadonnées d'instance	1065

Exemple Linux : valeur de l'index de lancement de l'AMI	1082
Documents d'identité d'instance	1087
Rôles d'identité d'instance	1152
Exécuter des commandes au lancement	1154
Comment Amazon EC2 gère les données utilisateur pour les instances Linux	1154
Comment Amazon EC2 gère les données utilisateur pour les instances Windows	1165
Connectez-vous à votre instance EC2	1181
Connectez-vous à votre instance Linux	1181
Connexion à votre instance Windows	1258
Connexion à l'aide du Gestionnaire de session	1271
Connectez-vous à l'aide du point de terminaison EC2 Instance Connect	1273
Connexion de votre instance à une ressource	1300
Identification d'instances	1346
Inspecter l'UUID du système	1346
Inspecter l'identificateur de génération de machine virtuelle du système	1348
Gérer les paramètres du système	1354
Réglage de l'heure	1354
Contrôle des états du processeur	1378
Optimiser les options d'UC	1380
AMD SEV-SNP	1505
Ajouter des composants du système Windows	1511
Gérer les utilisateurs du système Linux	1517
Définissez le mot de passe de l'administrateur Windows	1521
Gérer les pilotes de périphériques	1523
Installer les pilotes NVIDIA	1523
Installer les pilotes AMD	1561
Pilotes PV pour Windows	1570
AWS Pilotes Windows NVMe	1607
Configuration des instances Windows	1615
Configuration des agents de lancement Windows	1615
Utiliser EC2 Fast Launch pour Windows	1786
Utiliser les accélérateurs Elastic Graphics sous Windows	1811
Installez WSL sous Windows	1833
Mise à niveau des instances Windows	1835
Effectuer une mise à niveau sur place	1836
Effectuer une mise à niveau automatique	1841

Migrer vers un type d'instance de génération actuelle	1852
Migration de Microsoft SQL Server depuis Windows vers Linux	1862
Résoudre les problèmes d'une mise à niveau	1863
Flottes	1864
EC2 Fleet	1865
Limites flotte EC2	1867
instances à capacité extensible	1867
Types de demande flotte EC2	1868
Stratégies de configuration d'une flotte EC2	1896
Travailler avec Flottes EC2	1937
Parc d'instances Spot	1965
Types de demande de parc d'instances Spot	1965
Stratégies de configuration d'un parc d'instances Spot	1966
Utilisation de flottes d'instances Spot	2006
CloudWatch métriques pour Spot Fleet	2042
Scalabilité automatique du parc d'instances Spot	2046
Surveiller des événements de flotte	2056
Types d'événements de flotte EC2	2057
Types d'événements de parc d'instances Spot	2064
Créer des EventBridge règles	2070
Didacticiels	2082
Didacticiel : Utiliser une flotte EC2 avec pondération des instances	2082
Didacticiel : Utiliser une flotte EC2 avec la capacité à la demande comme capacité principale	2086
Didacticiel : Lancer des instances à la demande en utilisant les réservations de capacité ciblées	2088
Tutoriel : Lancer des instances dans des blocs de capacité	2095
Didacticiel : utiliser un flotte d'instances EC2 avec pondération des instances	2097
Exemples de configuration	2100
Exemples de configuration d'une flotte EC2	2101
Exemples de configuration d'un parc d'instances Spot	2121
Quotas liés aux flottes	2140
Demander une augmentation de quota pour la capacité cible	2142
Contrôle	2143
Surveillance automatique et surveillance manuelle	2144
Outils de surveillance automatique	2145

Outils de surveillance manuelle	2146
Bonnes pratiques de surveillance	2147
Surveiller le statut de vos instances	2147
Contrôles de statut des instances	2148
Événements de changement d'état	2157
Événements planifiés	2160
Surveillez vos instances à l'aide de CloudWatch	2193
Alarmes d'instance	2194
Activer la surveillance détaillée	2195
Répertorier les métriques disponibles	2198
Installation et configuration de l' CloudWatch agent	2224
Obtenir les statistiques des métriques	2228
Graphique de métriques	2238
Créer une alarme	2239
Créer des alarmes qui arrêtent, finissent, redémarrent ou récupèrent une instance	2240
Automatisez l'utilisation EventBridge	2254
Types d'événements Amazon EC2	2255
Enregistrez les appels d'API en utilisant CloudTrail	2256
Informations sur l'API Amazon EC2 dans CloudTrail	2256
Comprendre les entrées du fichier journal de l'API Amazon EC2	826
Auditez les connexions via EC2 Instance Connect	2259
Surveillez vos applications .NET et SQL Server.	2260
Suivi de votre utilisation de l'offre gratuite	2261
Mise en réseau	2265
Régions et zones	2266
Régions	2267
Zones de disponibilité	2274
Zones locales	2278
Zones Wavelength	2281
AWS Outposts	2284
Adressage IP des instances	2286
Adresses IPv4 privées	2287
Adresses IPv4 publiques	2288
Optimisation des adresses IPv4 publiques	2290
Adresses IP Elastic (IPv4)	2291
Adresses IPv6	2291

Utiliser les adresses IPv4 pour vos instances	2293
Utiliser les adresses IPv6 pour vos instances	2296
Plusieurs adresses IP	2299
Plusieurs adresses IPv4 privées pour Windows	2309
Noms d'hôtes d'instance EC2	2317
Adresses lien-local	2317
Types de noms d'hôte d'instance	2318
Types de noms d'hôte EC2	2318
Où vous voyez le nom de la ressource et le nom d'adresse IP	2320
Comment décider s'il faut choisir le nom de la ressource ou le nom IP	2322
Modifier le type de nom d'hôte et les configurations de noms d'hôte DNS	2323
Fourniture de vos propres adresses IP	2325
Définitions BYOIP	2326
Exigences et quotas	2327
Conditions préalables à l'onboarding	2328
Intégrer votre BYOIP	2336
Utiliser votre plage d'adresses	2341
Valider votre BYOIP	2342
Disponibilité par région	2347
Disponibilité de la zone locale	2347
En savoir plus	2347
Adresses IP Elastic	2348
Tarification des adresses IP Elastic	2348
Principes de base d'une adresse IP Elastic	2348
Utiliser des adresses IP Elastic	2350
Quota appliqué aux adresses IP Elastic	2366
Interfaces réseau	2367
Notions fondamentales concernant l'interface réseau	2368
Cartes réseau	2370
Adresses IP par interface réseau et par type d'instance	2372
Utiliser des interfaces réseau	2373
Meilleures pratiques pour la configuration des interfaces réseau	2385
Scénarios pour les interfaces réseau	2388
Interfaces réseau gérées par demandeur	2392
Attribuer des préfixes	2394
Bande passante réseau	2411

Bande passante d'instance disponible	2412
Contrôle de la bande passante de l'instance	2414
Réseaux améliorés	2414
Prise en charge de la mise en réseau améliorée	2415
Elastic Network Adapter (ENA)	2416
ENA Express	2447
Intel 82599 VF	2470
Métriques des performances réseau	2483
Résoudre les problèmes liés à l'ENA sous Linux	2494
Résoudre les problèmes liés au pilote Windows ENA	2509
Amélioration de la latence réseau sur les instances Linux	2531
Considérations relatives aux performances de Nitro	2535
Optimisation des performances réseau sur les instances Windows	2543
Elastic Fabric Adapter	2545
Principes de base EFA	2546
Interfaces et bibliothèques prises en charge	2548
Types d'instance pris en charge	2548
Systèmes d'exploitation pris en charge	2549
Restrictions liées à EFA	2550
Tarification EFA	2551
Commencer à utiliser les instances P5 et EFA	2551
Commencer avec EFA et MPI	2555
Commencer avec EFA et NCCL	2573
Travailler avec EFA	2614
Surveillez un EFA	2618
Vérification du programme d'installation EFA à l'aide d'un total de contrôle	2619
Topologie d'instance	2630
Comment ça marche	2631
Prérequis	2635
Exemples	2637
Groupes de placement	2649
Stratégies de placement	2649
Règles et limitations	2653
Utilisation des groupes de placement	2656
Partager un groupe de placement	2670
Groupes de placement sur AWS Outposts	2676

MTU réseau	2677
Trames jumbo (MTU de 9001)	2678
Détection de la MTU du chemin	2679
Vérifier la MTU du chemin entre deux hôtes	2680
Vérifiez le MTU de votre instance	2682
Définissez le MTU pour votre instance	2684
Dépannage	2686
Clouds privés virtuels	2686
Vos VPC par défaut	2687
Création de VPC supplémentaires	2687
Accès à Internet depuis vos instances	2689
Sous-réseaux partagés	2689
Sous-réseaux IPv6 uniquement	2690
Sécurité	2691
Protection des données	2692
Sécurité des données Amazon EBS	2693
Chiffrement au repos	2694
Chiffrement en transit	2695
Sécurité de l'infrastructure	2697
Isolement de réseau	2698
Isolation sur les hôtes physiques	2698
Contrôle du trafic réseau	2699
Résilience	2701
Validation de conformité	2702
Identity and Access Management	2704
Accès réseau à votre instance	2704
Attributs d'autorisation Amazon EC2	2705
IAM et Amazon EC2	2705
Stratégies IAM	2707
AWS politiques gérées	2781
Rôles IAM	2785
AWS PrivateLink	2803
Création d'un point de terminaison d'un VPC d'interface	2804
Créer une politique de point de terminaison	2804
Gestion des mises à jour	2806
Bonnes pratiques de sécurité pour les instances Windows	2806

Bonnes pratiques de sécurité de haut niveau	2807
Gestion des mises à jour	2808
Gestion de la configuration	2810
Gestion des modifications	2811
Audit et responsabilité pour les instances Windows Amazon EC2	2812
Paires de clés	2813
Création d'une paire de clés	2815
Baliser une paire de clés	2823
Décrivez vos paires de clés	2826
Supprimer votre paire de clés	2834
Ajouter ou supprimer une clé publique sur votre instance Linux	2835
Vérifier l'empreinte	2837
Groupes de sécurité	2840
Règles des groupes de sécurité	2842
Suivi de la connexion	2844
Groupes de sécurité par défaut et personnalisés	2850
Utiliser des groupes de sécurité	2852
Règles de groupe de sécurité pour différents cas d'utilisation	2863
NitroTPM	2871
Considérations	2872
Prérequis	2872
Créer une AMI Linux pour la prise en charge de NitroTPM	2874
Vérifiez si une AMI est activée pour NitroTPM	2875
Activer ou arrêter l'utilisation de NitroTPM sur une instance	2876
Récupérez la clé d'approbation publique	2878
Credential Guard pour les instances Windows	2880
Prérequis	2880
Lancer une instance prise en charge	2881
Désactiver l'intégrité de la mémoire	2882
Activez Credential Guard	2883
Vérifiez que Credential Guard est en cours d'exécution	2885
Stockage	2887
Amazon EBS	2888
Stockage d'instances	2889
Volume du stockage d'instances et durée de vie des données	2890
Volumes de stockage d'instances	2893

Ajouter des volumes de stockage d'instance	2895
Volumes de stockage d'instance SSD	2902
Volumes d'échange de stockage d'instance pour les instances Linux	2906
Optimisation des performances du disque sur les instances Linux	2910
Stockage de fichiers	2912
Amazon S3	2912
Amazon EFS	2915
Amazon FSx	2919
Cache de fichiers Amazon	2925
Limites de volume d'instance	2926
Limites de volume pour les instances créées sur le système Nitro	2926
Limites de volume pour les instances basées sur Xen	2929
volume du périphérique racine	2930
Type de volume racine	2930
Choisissez une AMI Linux par type de volume racine	2933
Déterminez le type de périphérique racine de votre instance Linux	2934
Modifier le volume racine pour qu'il persiste	2935
Modifier la taille initiale du volume racine	2939
Remplacer un volume racine	2940
Noms d'appareil	2952
Noms d'appareil disponibles	2953
Considérations sur les noms d'appareil	2955
Mappages de périphériques de stockage en mode bloc	2957
Concepts de mappage de périphérique de stockage en mode bloc	2957
Mappage de périphérique de stockage en mode bloc d'une AMI	2962
Mappage de périphérique de stockage en mode bloc d'une instance	2966
Mapper des disques sur des volumes	2974
Référencer les volumes NVMe	2975
Référencer les volumes	2981
Instantanés Windows VSS EBS	2990
Qu'est-ce qu' VSS ?	2991
Prérequis	2993
Créer des instantanés VSS	3010
Résoudre les problèmes liés aux instantanés EBS basés sur Windows VSS	3021
Restaurer des volumes à partir d'instantanés VSS	3027
Historique des versions	3027

Prévention de l'écriture déchirée pour les instances Linux	3031
Tarification	3032
Tailles de bloc et alignements des limites de blocs pris en charge	3032
Prérequis	3033
Vérifier la prise en charge et la configuration de la prévention des écritures déchirées	3033
Configuration de votre pile logicielle pour empêcher les écritures déchirées	3035
Ressources et balises	3038
Corbeille	3038
Fonctionnement	3039
Ressources prises en charge	3040
Considérations	3041
Quotas	3044
Services connexes	3044
Tarification	3045
Autorisations IAM requises	3045
Utiliser des règles de rétention	3050
Utiliser des ressources dans la corbeille	3066
Surveiller la corbeille	3076
Emplacements des ressources	3096
ID de ressource	3097
Lister et filtrer vos ressources	3098
Étapes de la console	3098
Étapes de la CLI et de l'API	3105
Vue globale (entre régions)	3108
Global View	3108
Baliser vos ressources	3112
Principes de base des balises	3113
Étiqueter vos ressources	3114
Restrictions liées aux balises	3119
Gestion des balises et des accès	3120
Baliser vos ressources pour facturation	3120
Utiliser des balises à l'aide de la console	3121
Utiliser des balises à l'aide de la ligne de commande	3127
Utiliser les identifications d'instance dans les métadonnées d'instance	3132
Ajoutez des balises à une ressource à l'aide de CloudFormation	3135
Quotas de service	3137

Afficher vos quotas actuels	3137
Demander une augmentation	3138
Restriction sur les e-mails envoyés à l'aide du port 25	3139
Dépannage	3140
Problèmes courants avec les instances Windows	3140
Les volumes EBS ne s'initialisent pas sur Windows Server 2016 et 2019	3141
Démarrer une instance Windows EC2 en mode de restauration des services d'annuaire (DSRM)	3142
L'instance perd la connectivité réseau ou les tâches programmées ne s'exécutent pas au moment prévu	3145
Impossible d'obtenir la sortie de la console	3146
Windows Server 2012 R2 non disponible sur le réseau	3146
Collision de signature de disque	3147
Messages courants avec les instances Windows	3148
« Le mot de passe n'est pas disponible »	3149
« Mot de passe pas encore disponible »	3150
« Récupération du mot de passe Windows impossible »	3150
« En attente du service de métadonnées »	3151
« L'activation de Windows est impossible »	3155
« Windows n'est pas authentique (0x80070005) »	3157
« Aucun serveur de licences Terminal Server n'est disponible pour fournir une licence » ...	3157
« Certains paramètres sont gérés par votre organisation »	3158
Résoudre les problèmes de lancement	3159
Nom de périphérique non valide	3159
Dépassement de la limite d'instance	3160
Capacité d'instance insuffisante	3161
La configuration demandée n'est actuellement pas prise en charge. Consultez la documentation pour voir les configurations prises en charge.	3162
Mise hors service immédiate de l'instance	3162
Autorisations insuffisantes	3164
Utilisation élevée du processeur peu après le démarrage de Windows (instances Windows uniquement)	3165
Connectez-vous à votre instance Linux	3166
Causes courantes des problèmes de connexion	3166
Erreur de connexion à votre instance : connexion expirée	3169
Erreur : impossible de charger la clé... Attente : N'IMPORTE QUELLE CLÉ PRIVÉE	3172

Erreur : clé de l'utilisateur non reconnue par le serveur	3173
Erreur : autorisation refusée ou connexion fermée par [instance] port 22	3175
Erreur : fichier de clé privée non protégé	3178
Erreur : La clé privée doit commencer par « ----BEGIN RSA PRIVATE KEY---- » et se terminer par « ----END RSA PRIVATE KEY---- »	3179
Erreur : le serveur a refusé notre clé ou Aucune méthode d'authentification prise en charge disponible	3180
Impossible d'envoyer une commande ping à l'instance	3181
Erreur : le serveur a fermé la connexion réseau de manière inopinée	3181
Erreur : échec de la validation de la clé d'hôte pour EC2 Instance Connect	3182
Impossible de se connecter à une instance Ubuntu à l'aide de EC2 Instance Connect	3184
J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Linux ?	3184
Connexion à votre instance Windows	3192
Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant	3193
Erreur lors de l'utilisation du client RDP macOS	3197
RDP affiche un écran noir au lieu du bureau	3197
Impossible de se connecter à distance à une instance avec un utilisateur autre qu'un administrateur	3198
Résolution des problèmes de bureau à distance à l'aide de AWS Systems Manager	3198
Activation du Bureau à distance sur une instance EC2 avec le Registre à distance	3202
J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Windows ?	3204
Réinitialisation d'un mot de passe administrateur Windows perdu ou expiré	3204
Réinitialiser à l'aide d'EC2Launch v2	3206
Réinitialisation d'EC2Config	3211
Réinitialiser à l'aide d'EC2Launch	3218
Résolution d'un problème d'instance inaccessible	3223
Redémarrage d'instance	3224
Sortie de la console de l'instance	3224
Création d'une capture d'écran d'une instance inaccessible	3225
Captures d'écran courantes pour les instances Windows	3227
Récupération d'instance en cas de plantage de l'ordinateur hôte	3237
Arrêter votre instance	3237
Forcer l'arrêt de l'instance	3238
Créer une instance de remplacement	3239
Résilier une instance	3241
Mise hors service immédiate de l'instance	3241

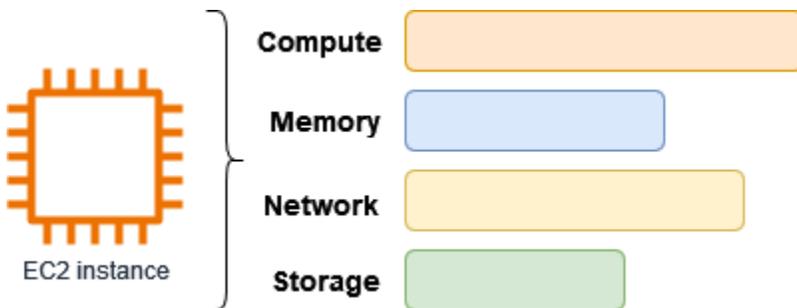
Mise à fin d'instance retardée	3241
Instance terminée toujours affichée	3242
Erreur : il se peut que l'instance ne soit pas résiliée. Modifier son attribut d'instance « désactiver ApiTermination »	3242
instances lancées ou terminées automatiquement	3242
Échec des vérifications d'état sous Linux	3243
Examen des informations de contrôle de statut	3244
Récupération des journaux système	3245
Résoudre les erreurs du journal système pour les instances Linux	3245
Mémoire insuffisante : processus d'arrêt	3247
ERROR: mmu_update failed (la mise à jour de la gestion de la mémoire a échoué)	3248
Erreur d'E/S (échec du périphérique de stockage en mode bloc)	3249
I/O ERROR: neither local nor remote disk (le périphérique de stockage en mode bloc distribué ne fonctionne plus)	3251
request_module: runaway loop modprobe (modprobe en boucle sur le noyau hérité sur des versions Linux plus anciennes)	3252
« FATAL: kernel too old » et « fsck: No such file or directory while trying to open / dev » (décalage entre le noyau et l'AMI)	3253
« FATAL : Impossible de charger /lib/modules » ou « BusyBox » (modules de noyau manquants)	3254
ERROR Invalid kernel (noyau incompatible EC2)	3256
fsck : aucun fichier ou répertoire de ce type lors de la tentative d'ouverture... (système de fichiers non trouvé)	3257
General error mounting filesystems (Montage en échec)	3260
VFS: Unable to mount root fs on unknown-block (le système de fichiers racine ne correspond pas)	3262
Erreur : Unable to determine major/minor number of root device... (décalage du système de fichiers/périphérique racine)	3263
XENBUS : Device with no driver...	3265
... days without being checked, check forced (Contrôle du système de fichiers nécessaire)	3266
fsck a échoué à l'état de sortie... (périphérique manquant)	3267
Invite GRUB (grubdom>)	3268
Mise en service de l'interface eth0 : l'adresse MAC du périphérique eth0 est différente de celle attendue, ignorer. (Adresse MAC codée de manière irréversible)	3271
Impossible de charger la politique SELinux. L'appareil est en mode d'exécution. Arrêt maintenant. (Erreur de configuration SELinux)	3273

XENBUS: Timeout connecting to devices (délai d'attente Xenbus)	3275
Résoudre les problèmes liés au démarrage d'une instance Linux à partir d'un volume incorrect	3276
Résoudre les problèmes liés à Sysprep	3278
EC2Rescue for Linux	3279
Installer EC2Rescue pour Linux	3280
(Facultatif) Vérification de la signature de EC2Rescue pour Linux	3281
Travailler avec EC2Rescue pour Linux	3285
Développer des modules EC2Rescue	3287
EC2Rescue for Windows Server	3295
Utiliser l'interface graphique	3295
Utiliser la ligne de commande	3302
Utiliser Systems Manager	3311
EC2 Serial Console	3315
Prérequis	3315
Configurer l'accès à l'EC2 Serial Console	3323
Connexion à l'EC2 Serial Console	3332
Déconnexion de l'EC2 Serial Console	3342
Résolution des problèmes de votre instance à l'aide de l'EC2 Serial Console	3343
Envoi d'une interruption de diagnostic	3353
Types d'instance pris en charge	3354
Prérequis	3354
Envoi d'une interruption de diagnostic	3358
Historique de la documentation	3359
Historique pour 2018 et les années antérieures	3389
.....	mmmcdxvii

Présentation d'Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) offre une capacité de mise à l'échelle à la demande dans le cloud Amazon Web Services (AWS). L'utilisation d'Amazon EC2 réduit les coûts de matériel, ce qui vous permet de développer et de déployer des applications plus rapidement. Vous pouvez utiliser Amazon EC2 pour lancer autant de serveurs virtuels que nécessaire, configurer la sécurité et les réseaux, et gérer le stockage. Vous pouvez ajouter de la capacité (augmenter) pour gérer les tâches lourdes en termes de calcul, telles que les processus mensuels ou annuels, ou les pics de trafic sur les sites web. Lorsque l'utilisation diminue, vous pouvez de nouveau restreindre la capacité (réduire).

Une instance EC2 est un serveur virtuel dans le AWS cloud. Lorsque vous lancez une instance EC2, le type d'instance que vous spécifiez détermine le matériel disponible pour votre instance. Chaque type d'instance offre un équilibre différent entre les ressources de calcul, de mémoire, de réseau et de stockage. Pour plus d'informations, consultez le guide des [types d'instances Amazon EC2](#).



Fonctionnalités d'Amazon EC2

Amazon EC2 offre les fonctionnalités de haut niveau suivantes :

instances

Serveurs virtuels.

Amazon Machine Images (AMI)

Modèles préconfigurés pour vos instances qui regroupent les packages des composants dont vous avez besoin pour votre serveur (y compris le système d'exploitation et les logiciels supplémentaires).

Types d'instances

Diverses configurations de CPU, de mémoire, de stockage, de capacité réseau et de matériel graphique pour vos instances.

Volumes Amazon EBS

Volumes de stockage permanents pour vos données à l'aide d'Amazon Elastic Block Store (Amazon EBS).

Volumes de stockage d'instances

Volumes de stockage pour les données temporaires qui sont supprimées lorsque vous arrêtez, mettez en veille prolongée ou résiliez votre instance.

Paires de clés

Informations de connexion sécurisées pour vos instances. AWS stocke la clé publique et vous stockez la clé privée dans un endroit sécurisé.

Groupes de sécurité

Un pare-feu virtuel qui vous permet de spécifier les protocoles, les ports et les plages d'adresses IP source qui peuvent atteindre vos instances, ainsi que les plages d'adresses IP de destination auxquelles vos instances peuvent se connecter.

Amazon EC2 prend en charge le traitement, le stockage et la transmission des données de cartes bancaires par un commerçant ou un fournisseur de services et a été validé comme étant conforme à la norme PCI (Payment Card Industry) DSS (Data Security Standard). Pour plus d'informations sur la norme PCI DSS, notamment sur la manière de demander une copie du Package de AWS conformité PCI, consultez la section [PCI DSS niveau 1](#).

Services connexes

Services à utiliser avec Amazon EC2

Vous pouvez en utiliser d'autres Services AWS avec les instances que vous déployez à l'aide d'Amazon EC2.

[Amazon EC2 Auto Scaling](#)

Permet de s'assurer que vous disposez du nombre adéquat d'instances Amazon EC2 pour gérer la charge de votre application.

[AWS Backup](#)

Automatisez la sauvegarde de vos instances Amazon EC2 et des volumes Amazon EBS qui leur sont attachés.

[Amazon CloudWatch](#)

Surveillez vos instances et vos volumes Amazon EBS.

[Elastic Load Balancing](#)

Répartissez automatiquement le trafic applicatif entrant sur plusieurs instances.

[Amazon GuardDuty](#)

Détectez l'utilisation potentiellement non autorisée ou malveillante de vos instances EC2.

[EC2 Image Builder](#)

Automatisez la création, la gestion et le déploiement d'images personnalisées, sécurisées et de up-to-date serveur.

[AWS Launch Wizard](#)

Dimensionnez, configurez et déployez des AWS ressources pour des applications tierces sans avoir à identifier et à provisionner manuellement AWS des ressources individuelles.

[AWS Systems Manager](#)

Effectuez des opérations à grande échelle sur des instances EC2 grâce à cette solution end-to-end de gestion sécurisée.

Services informatiques supplémentaires

Vous pouvez lancer des instances à l'aide d'un autre service de AWS calcul au lieu d'utiliser Amazon EC2.

[Amazon Lightsail](#)

Créez des sites Web ou des applications Web à l'aide d'Amazon Lightsail, une plateforme cloud qui fournit les ressources dont vous avez besoin pour déployer rapidement votre projet, à un prix mensuel bas et prévisible. [Pour comparer Amazon EC2 et Lightsail, consultez Amazon Lightsail ou Amazon EC2.](#)

[Amazon Elastic Container Service \(Amazon ECS\)](#)

Déployez, gérez et faites évoluer des applications conteneurisées sur un cluster d'instances EC2. Pour plus d'informations, consultez la section [Choix d'un service de AWS conteneur](#).

[Amazon Elastic Kubernetes Service \(Amazon EKS\)](#)

Exécutez vos applications Kubernetes sur AWS. Pour plus d'informations, consultez la section [Choix d'un service de AWS conteneur](#).

Accès à Amazon EC2

Vous pouvez créer et gérer vos instances Amazon EC2 à l'aide des interfaces suivantes :

Console Amazon EC2

Une interface web simple pour créer et gérer les instances et les ressources Amazon EC2. Si vous avez créé un AWS compte, vous pouvez accéder à la console Amazon EC2 en vous connectant AWS Management Console et en sélectionnant EC2 sur la page d'accueil de la console.

AWS Command Line Interface

Vous permet d'interagir avec les AWS services à l'aide des commandes de votre interface de ligne de commande. Elle est prise en charge sur Windows, Mac et Linux. Pour plus d'informations sur l' AWS CLI , consultez le [Guide de l'utilisateur AWS Command Line Interface](#). Vous trouverez les commandes Amazon EC2 dans la [Référence des commandes AWS CLI](#) (français non garanti).

AWS CloudFormation

Amazon EC2 prend en charge la création de ressources avec AWS CloudFormation. Vous créez un modèle, au format JSON ou YAML, qui décrit vos AWS ressources, fournit AWS CloudFormation et configure ces ressources pour vous. Vous pouvez réutiliser vos CloudFormation modèles pour fournir les mêmes ressources plusieurs fois, que ce soit dans la même région et le même compte ou dans plusieurs régions et comptes. Pour plus d'informations sur les types de ressources et les propriétés prises en charge pour Amazon EC2, consultez [Référence des types de ressources EC2](#) (français non garanti) dans le Guide de l'utilisateur AWS CloudFormation .

AWS SDK

Si vous préférez créer des applications à l'aide d'API spécifiques à un langage plutôt que de soumettre une demande via HTTP ou HTTPS, AWS fournit des bibliothèques, des exemples de code, des didacticiels et d'autres ressources pour les développeurs de logiciels. Ces bibliothèques offrent des fonctions de base qui automatisent les tâches telles que la signature cryptographique des demandes, les nouvelles tentatives de demande et la gestion des réponses d'erreur. Vous pouvez ainsi démarrer plus facilement. Pour en savoir plus, consultez la section [Outils pour créer sur AWS](#).

AWS Tools for PowerShell

Un ensemble de PowerShell modules basés sur les fonctionnalités exposées par le AWS SDK for .NET. Les outils vous PowerShell permettent de scripter des opérations sur vos AWS ressources à partir de la ligne de PowerShell commande. Consultez le [AWS Tools for Windows PowerShell Guide de l'utilisateur](#) pour démarrer. Vous trouverez les cmdlets pour Amazon EC2 dans la [Référence des cmdlets AWS Tools for PowerShell](#) (français non garanti).

API de requête

Amazon EC2 fournit une API de requête. Ces requêtes sont des requêtes HTTP ou HTTPS qui utilisent les verbes HTTP GET ou POST et un paramètre de requête nommé `Action`. Pour plus d'informations sur les actions d'API pour Amazon EC2, consultez [Actions](#) dans le Amazon EC2 API Reference.

Tarifcation pour Amazon EC2

Amazon EC2 fournit les options suivantes :

Offre gratuite

Vous pouvez commencer à utiliser Amazon EC2 gratuitement. Pour explorer les options de l'offre gratuite, consultez [Offre gratuite d'AWS](#).

On-Demand instances

Payez les instances que vous utilisez à la seconde, avec un minimum de 60 secondes, sans engagement à long terme ou paiement initial.

Savings Plans

Vous pouvez réduire les coûts de Amazon EC2 en vous engageant pour une utilisation continue, en USD par heure, pour une durée de 1 à 3 ans.

Reserved instances

Vous pouvez réduire les coûts de Amazon EC2 en vous engageant pour une configuration d'instance spécifique, incluant le type et la région, pour une durée de 1 à 3 ans.

Spot instances

Demande d'instances EC2 inutilisées, ce qui peut réduire vos coûts de Amazon EC2 de façon considérable.

Hôtes dédiés

Réduisez vos coûts en utilisant un serveur EC2 physique entièrement dédié à votre usage, soit à la demande, soit dans le cadre d'un Savings Plan. Vous pouvez utiliser vos licences logicielles existantes liées au serveur et obtenir de l'aide pour répondre aux exigences de conformité.

On-Demand Capacity Reservations

Réservez de la capacité de calcul pour vos instances EC2 dans une zone de disponibilité spécifique pour n'importe quelle durée.

Facturation à la seconde

Supprime de votre facture le coût des minutes et des secondes inutilisées.

Pour obtenir une liste complète des frais et des prix d'Amazon EC2 et plus d'informations sur les modèles d'achat, consultez [Tarification Amazon EC2](#).

Estimations, facturation et optimisation des coûts

Pour créer des estimations pour vos cas AWS d'utilisation, utilisez le [AWS Pricing Calculator](#).

Pour estimer le coût de la transformation des charges de travail Microsoft vers une architecture moderne utilisant des services open source et cloud natifs déployés AWS, utilisez le [calculateur de AWS modernisation pour les charges de travail Microsoft](#).

Pour consulter votre facture, dirigez-vous vers le Tableau de bord de gestion des coûts et de la facturation dans la [console AWS Billing and Cost Management](#). Votre facture contient des liens vers les rapports d'utilisation qui fournissent des détails sur votre facture. Pour en savoir plus

sur la facturation des AWS comptes, consultez le [guide de l'utilisateur AWS de Billing and Cost Management](#).

Si vous avez des questions concernant la AWS facturation, les comptes et les événements, [contactez le AWS Support](#).

Pour calculer le coût d'un exemple d'environnement alloué, consultez le [Centre d'optimisation des coûts du Cloud](#). Lorsque vous calculez le coût d'un environnement alloué, n'oubliez pas d'inclure les coûts accessoires tels que le stockage d'instantanés pour les volumes EBS.

Vous pouvez optimiser le coût, la sécurité et les performances de votre AWS environnement à l'aide de [AWS Trusted Advisor](#).

Vous pouvez l'utiliser AWS Cost Explorer pour analyser le coût et l'utilisation de vos instances EC2. Vous pouvez consulter les données des 13 derniers mois et prévoir le montant que vous êtes susceptible de dépenser au cours des 12 prochains mois. Pour plus d'informations, consultez la section [Analyse de vos coûts AWS Cost Explorer](#) dans le guide de AWS Cost Management l'utilisateur.

Ressources

- [Fonctionnalités d'Amazon EC2](#)
- [AWS Re : Publier](#)
- [AWS Générateur de compétences](#)
- [AWS Support](#)
- [Tutoriels pratiques](#)
- [Hébergement Web](#)
- [Windows activé AWS](#)

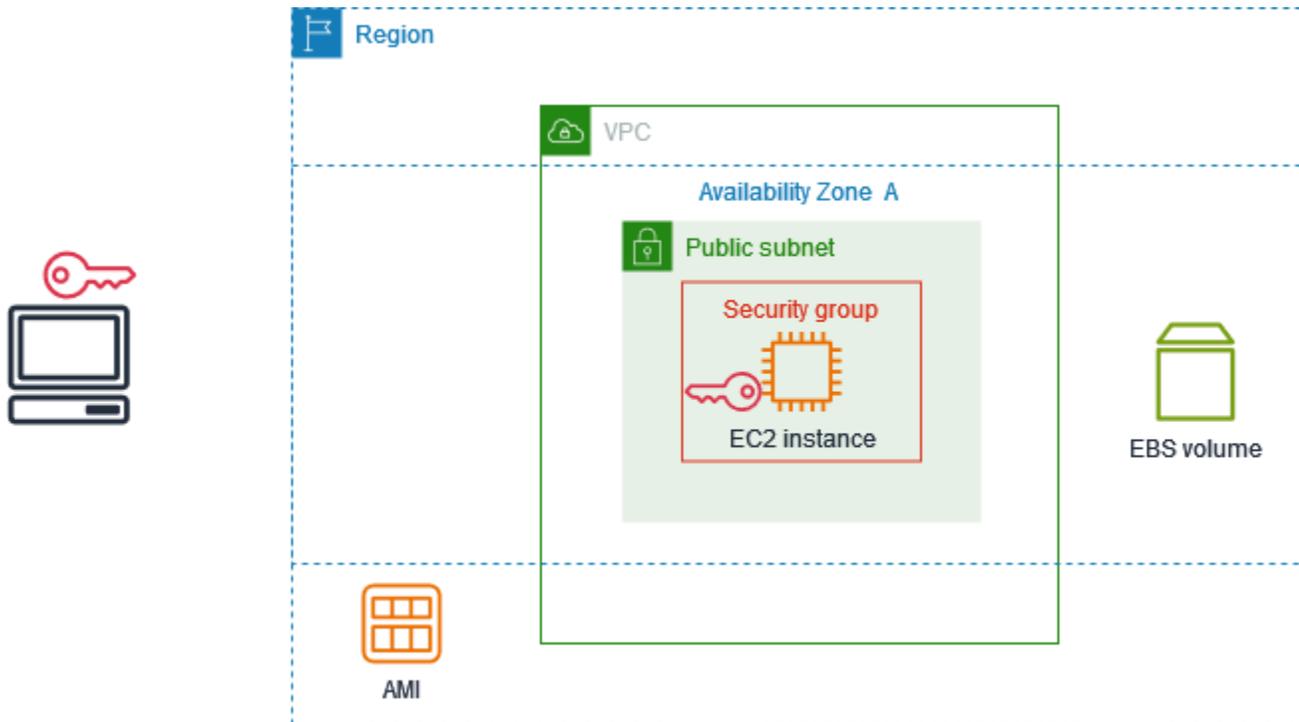
Mise en route avec Amazon EC2

Utilisez ce tutoriel pour commencer avec Amazon Elastic Compute Cloud (Amazon EC2). Vous allez apprendre à lancer une instance EC2 et à vous y connecter. Une instance est un serveur virtuel dans le AWS Cloud. Avec Amazon EC2, vous pouvez installer et configurer le système d'exploitation et les applications qui s'exécutent sur votre instance.

Présentation

Le schéma suivant montre les principaux composants que vous allez utiliser dans ce didacticiel :

- Une image : modèle contenant le logiciel à exécuter sur votre instance, tel que le système d'exploitation.
- Une paire de clés : ensemble d'informations d'identification de sécurité que vous utilisez pour prouver votre identité lorsque vous vous connectez à votre instance. La clé publique se trouve sur votre instance et la clé privée sur votre ordinateur.
- Un réseau — Un cloud privé virtuel (VPC) est un réseau virtuel dédié à votre. Compte AWS Pour vous aider à démarrer rapidement, votre compte est fourni avec un VPC par défaut dans chaque compte Région AWS, et chaque VPC par défaut possède un sous-réseau par défaut dans chaque zone de disponibilité.
- Un groupe de sécurité : agit comme un pare-feu virtuel pour contrôler le trafic entrant et sortant.
- Un volume EBS — Nous avons besoin d'un volume racine pour l'image. Vous pouvez éventuellement ajouter des volumes de données.



Coût de ce didacticiel

Lorsque vous vous inscrivez à AWS, vous pouvez commencer à utiliser Amazon EC2 en utilisant le [Niveau gratuit d'AWS](#). Si vous avez créé le vôtre il y a moins de 12 mois et que vous n'avez pas encore dépassé les avantages du niveau gratuit pour Amazon EC2, suivre ce didacticiel ne vous coûtera rien, car nous vous aidons à sélectionner les options incluses dans les avantages du niveau gratuit. Sinon, vous devrez payer les frais d'utilisation Amazon EC2 standard à partir du moment où vous lancez l'instance et jusqu'à ce que vous mettiez fin à celle-ci (ce qui constitue la tâche finale de ce tutoriel), même si elle reste inactive.

Pour obtenir des instructions permettant de déterminer si vous êtes éligible au niveau gratuit, consultez [the section called "Suivi de votre utilisation de l'offre gratuite"](#).

Tâches

- [Étape 1 : Lancer une instance](#)
- [Étape 2 : Connexion à l'instance](#)
- [Étape 3 : Nettoyage de votre instance](#)
- [Étapes suivantes](#)

Étape 1 : Lancer une instance

Vous pouvez lancer une instance EC2 à l'aide de la procédure AWS Management Console décrite dans la procédure suivante. Ce didacticiel est destiné à vous aider à lancer rapidement votre première instance dans le cadre des avantages du niveau gratuit. Il ne couvre donc pas toutes les options possibles.

Pour lancer une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation en haut de l'écran, nous affichons le courant Région AWS , par exemple l'Ohio. Vous pouvez utiliser la région sélectionnée ou éventuellement sélectionner une région plus proche de vous.
3. Dans le tableau de bord de la console EC2, dans le volet Launch instance, choisissez Launch instance.
4. Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom descriptif pour votre instance.
5. Sous Application and OS Images (Amazon Machine Image) (Images d'application et de système d'exploitation [Amazon Machine Image]), procédez comme suit :
 - a. Choisissez Quick Start, puis choisissez le système d'exploitation (OS) de votre instance. Pour votre première instance Linux, nous vous recommandons de choisir Amazon Linux.
 - b. Dans Amazon Machine Image (AMI), sélectionnez une AMI marquée comme éligible au niveau gratuit.
6. Sous Type d'instance, dans Type d'instancet2.micro, choisissez laquelle est éligible au niveau gratuit. Dans les régions où t2.micro il n'est pas disponible, t3.micro est éligible au niveau gratuit.
7. Sous Paire de clés (connexion), pour Nom de la paire de clés, choisissez une paire de clés existante ou choisissez Créer une nouvelle paire de clés pour créer votre première paire de clés.

Warning

Si vous choisissez Proceed without a key pair (non recommandé), vous ne pourrez pas vous connecter à votre instance à l'aide des méthodes décrites dans ce didacticiel.

8. Dans Paramètres réseau, notez que nous avons sélectionné votre VPC par défaut, sélectionné l'option permettant d'utiliser le sous-réseau par défaut dans une zone de disponibilité que nous avons choisie pour vous et configuré un groupe de sécurité avec une règle autorisant les connexions à votre instance depuis n'importe où. Pour votre première instance, nous vous recommandons d'utiliser les paramètres par défaut. Sinon, vous pouvez mettre à jour vos paramètres réseau comme suit :
 - (Facultatif) Pour utiliser un sous-réseau par défaut spécifique, choisissez Modifier, puis choisissez un sous-réseau.
 - (Facultatif) Pour utiliser un autre VPC, choisissez Modifier, puis choisissez un VPC existant. Si le VPC n'est pas configuré pour un accès public à Internet, vous ne pourrez pas vous connecter à votre instance.
 - (Facultatif) Pour restreindre le trafic de connexion entrant vers un réseau spécifique, choisissez Personnalisé au lieu de Anywhere, puis entrez le bloc CIDR pour votre réseau.
 - (Facultatif) Pour utiliser un autre groupe de sécurité, choisissez Sélectionner un groupe de sécurité existant, puis choisissez un groupe de sécurité existant. Si le groupe de sécurité n'a pas de règle autorisant le trafic de connexion depuis votre réseau, vous ne pourrez pas vous connecter à votre instance. Pour une instance Linux, vous devez autoriser le trafic SSH. Pour une instance Windows, vous devez autoriser le trafic RDP.
9. Sous Configurer le stockage, notez que nous avons configuré un volume racine mais aucun volume de données. Cela est suffisant à des fins de test.
10. Consultez un résumé de la configuration de votre instance dans le panneau Summary (Récapitulatif) et, lorsque vous êtes prêt, choisissez Launch instance (Lancer l'instance).
11. Si le lancement est réussi, choisissez l'ID de l'instance dans la notification de réussite pour ouvrir la page Instances et surveiller l'état du lancement.
12. Cochez la case correspondant à l'instance. L'état initial de l'instance est `pending`. Lorsque l'instance démarre, son statut passe à `running`. Choisissez l'onglet État et alarmes. Une fois que votre instance a passé ses vérifications d'état, elle est prête à recevoir des demandes de connexion.

Étape 2 : Connexion à l'instance

La procédure que vous utilisez dépend du système d'exploitation de l'instance. Si vous ne pouvez pas vous connecter à votre instance, consultez [Résoudre les problèmes de connexion à votre instance Linux](#) pour obtenir de l'aide.

Instances Linux

Vous pouvez vous connecter à votre instance Linux à l'aide de n'importe quel client SSH. Si vous utilisez Windows sur votre ordinateur, ouvrez un terminal et exécutez la `ssh` commande pour vérifier qu'un client SSH est installé. Si la commande est introuvable, [installez OpenSSH](#) pour Windows.

Pour vous connecter à votre instance à l'aide de SSH

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance, puis choisissez Connecter.
4. Sur la page Connect to instance, sélectionnez l'onglet client SSH.
5. (Facultatif) Si vous avez créé une paire de clés lorsque vous avez lancé l'instance et téléchargé la clé privée (fichier `.pem`) sur un ordinateur exécutant Linux ou macOS, exécutez l'exemple de `chmod` commande pour définir les autorisations associées à votre clé privée.
6. Copiez l'exemple de commande SSH. Voici un exemple où *key-pair-name .pem est le nom* de votre fichier de clé privée, *ec2-user est le nom d'utilisateur* associé à l'image et la chaîne après le symbole `@` est le nom DNS public de l'instance.

```
ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
```

7. Dans une fenêtre de terminal de votre ordinateur, exécutez la `ssh` commande que vous avez enregistrée à l'étape précédente. Si le fichier de clé privée ne se trouve pas dans le répertoire actuel, vous devez spécifier le chemin complet vers le fichier clé dans cette commande.

Voici un exemple de réponse :

```
The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
(198-51-100-1)' can't be established.
ECDSA key fingerprint is 14UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

8. (Facultatif) Vérifiez que l'empreinte de l'alerte de sécurité correspond à l'empreinte de l'instance contenue dans la sortie de la console lorsque vous démarrez une instance pour la première fois. Pour obtenir le résultat de la console, choisissez Actions, Surveiller et dépanner, puis Obtenir le journal du système. Si les empreintes digitales ne correspondent pas, quelqu'un est peut-être en train de tenter une man-in-the-middle attaque. Si elles correspondent, passez à l'étape suivante.
9. Saisissez **yes**.

Voici un exemple de réponse :

```
Warning: Permanently added 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

instances Windows

Pour vous connecter à une instance Windows, vous devez récupérer le mot de passe administrateur initial et utiliser ce mot de passe lorsque vous vous connectez à votre instance via Remote Desktop. Il faut quelques minutes après le lancement de l'instance pour que ce mot de passe soit disponible.

Le nom d'utilisateur par défaut du compte administrateur dépend de la langue du système d'exploitation (OS) contenu dans l'AMI. Pour déterminer le nom d'utilisateur correct, identifiez la langue du système d'exploitation de votre AMI, puis choisissez le nom d'utilisateur correspondant. Par exemple, pour un système d'exploitation anglais, le nom d'utilisateur est `Administrator`, pour un système d'exploitation français, c'est le cas `Administrateur`, et pour un système d'exploitation portugais, c'est le cas `Administrador`. Si une version linguistique du système d'exploitation ne possède pas de nom d'utilisateur dans la même langue, choisissez-le `Administrator (Other)`. Pour plus d'informations, consultez la section [Noms localisés du compte administrateur sous Windows](#) sur le Microsoft TechNet Wiki.

Si vous avez joint votre instance à un domaine, vous pouvez vous connecter à votre instance à l'aide des autorisations de domaine que vous avez définies dans AWS Directory Service. Sur l'écran de connexion Bureau à distance, au lieu d'utiliser le nom de l'ordinateur local et le mot de passe généré, utilisez le nom d'utilisateur complet pour l'administrateur (par exemple, `corp.example.com\Admin`) et le mot de passe de ce compte.

Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [the section called "Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant"](#).

Pour vous connecter à votre instance de Windows en utilisant un client RDP

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance, puis choisissez Connecter.
4. Sur la page Connect to instance, sélectionnez l'onglet client RDP.

5. Dans Nom d'utilisateur, choisissez le nom d'utilisateur par défaut pour le compte administrateur. Le nom d'utilisateur que vous choisissez doit correspondre à la langue du système d'exploitation (OS) contenu dans l'AMI que vous avez utilisée pour lancer votre instance. S'il n'existe aucun nom d'utilisateur dans la même langue que votre système d'exploitation, choisissez Administrator (Other).
6. Choisissez Obtenir le mot de passe.
7. Sur la page Obtenir le mot de passe Windows, procédez comme suit :
 - a. Choisissez Télécharger le fichier de clé privée et accédez au fichier de clé privée (.pem) que vous avez spécifié lors du lancement de l'instance. Sélectionnez le fichier, puis choisissez Open (Ouvrir) pour copier tout le contenu du fichier dans cette page.
 - b. Choisissez Déchiffrer le mot de passe. La page Obtenir le mot de passe Windows se ferme et le mot de passe administrateur par défaut de l'instance apparaît sous Mot de passe, en remplacement du lien Obtenir le mot de passe affiché précédemment.
 - c. Copiez le mot de passe et enregistrez-le en lieu sûr. Vous en aurez besoin pour vous connecter à l'instance.
8. Sélectionnez Télécharger le fichier Bureau à distance. Lorsque vous avez terminé de télécharger le fichier, choisissez Annuler pour revenir à la page Instances. Accédez à votre répertoire de téléchargements et ouvrez le fichier RDP.
9. Vous pouvez obtenir un avertissement indiquant que l'éditeur de la connexion à distance est inconnu. Choisissez Se connecter pour vous connecter à votre instance.
10. Le compte d'administrateur est choisi par défaut. Collez le mot de passe que vous avez copié précédemment, puis cliquez sur OK.
11. En raison de la nature des certificat auto-signés, vous pouvez obtenir un avertissement indiquant que le certificat de sécurité ne peut pas être authentifié. Effectuez l'une des actions suivantes :
 - Si vous faites confiance au certificat, choisissez Oui pour vous connecter à votre instance.
 - [Windows] Avant de continuer, comparez l'empreinte numérique du certificat avec la valeur du journal système pour confirmer l'identité de l'ordinateur distant. Choisissez Afficher le certificat, puis sélectionnez Thumbprint dans l'onglet Détails. Comparez cette valeur à celle de RDPCERTIFICATE-THUMBPRINT la section Actions, Surveillance et résolution des problèmes, Obtenir le journal du système.
 - [Mac OS X] Avant de continuer, comparez l'empreinte du certificat avec la valeur du journal système pour confirmer l'identité de l'ordinateur distant. Choisissez Afficher le certificat, développez les détails, puis choisissez SHA1 Fingerprints. Comparez cette valeur à celle

de RDPCERTIFICATE-THUMBPRINT la section Actions, Surveillance et résolution des problèmes, Obtenir le journal du système.

Étape 3 : Nettoyage de votre instance

Une fois que vous avez fini avec l'instance que vous avez créée pour ce tutoriel, vous devez effectuer un nettoyage en mettant fin à l'instance. Si vous souhaitez exécuter d'autres opérations avec cette instance avant le nettoyage, consultez [Étapes suivantes](#).

Important

Mettre fin à une instance la supprime ; vous ne pouvez pas vous reconnecter à une instance une fois que vous y avez mis fin.

Si vous avez lancé une instance qui ne fait pas partie de la [Niveau gratuit d'AWS](#), cette instance ne vous est plus facturée dès que son statut passe à shutting down ou terminated. Pour conserver une instance pour l'utiliser ultérieurement, mais sans payer de frais, vous pouvez arrêter l'instance maintenant et la redémarrer plus tard. Pour plus d'informations, consultez [Arrêtez et démarrez les instances Amazon EC2](#).

Pour mettre fin à une instance

1. Dans le panneau de navigation, choisissez Instances. Sélectionnez l'instance dans la liste des instances.
2. Choisissez État de l'instance, Résilier l'instance.
3. Choisissez Résilier lorsque vous êtes invité à confirmer.

Amazon EC2 arrête et met fin à votre instance. Après que votre instance a pris fin, elle reste visible sur la console pendant un court instant, puis l'entrée est supprimée automatiquement. Vous ne pouvez pas supprimer vous-même l'instance résiliée de l'affichage de la console.

Étapes suivantes

Après avoir démarré votre instance, vous souhaitez peut-être explorer les étapes suivantes :

- Découvrez comment suivre votre utilisation de l'offre gratuite pour éviter les surprises liées à la facturation. Pour plus d'informations, consultez [the section called "Suivi de votre utilisation de l'offre gratuite"](#).
- Configurez une CloudWatch alarme pour vous avertir si votre utilisation dépasse le niveau gratuit. Pour plus d'informations, consultez la section [Suivi de votre utilisation du niveau AWS gratuit](#) dans le guide de AWS Billing l'utilisateur.
- Ajoutez un volume EBS. Pour plus d'informations, consultez la section [Créer un volume Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.
- Découvrez comment gérer à distance votre instance EC2 à l'aide de la commande Run. Pour plus d'informations, consultez [AWS Systems Manager Run Command](#) dans le AWS Systems Manager Guide de l'utilisateur.
- En savoir plus sur les options d'achat d'instances. Pour plus d'informations, consultez [Options d'achat d'instance](#).
- Obtention de conseils sur les types d'instances Pour plus d'informations, voir [Obtention de recommandations sur le type d'instance pour une nouvelle charge de travail](#).

Bonnes pratiques relatives à Amazon EC2.

Pour tirer le meilleur parti d'Amazon EC2, nous vous recommandons de suivre les bonnes pratiques suivantes.

Sécurité

- Gérez l'accès aux AWS ressources et aux API en utilisant la fédération d'identité avec un fournisseur d'identité et des rôles IAM dans la mesure du possible. Pour plus d'informations, consultez [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM.
- Implémentez les règles les moins permissives pour votre groupe de sécurité. Pour plus d'informations, veuillez consulter [Règles des groupes de sécurité](#).
- Corrigez, mettez à jour et sécurisez régulièrement le système d'exploitation et les applications de votre instance. Pour plus d'informations, consultez [Gestion des mises à jour](#). Pour les directives spécifiques aux systèmes d'exploitation Windows, voir [Bonnes pratiques de sécurité pour les instances Windows](#).
- Utilisez Amazon Inspector pour détecter et analyser automatiquement les vulnérabilités logicielles et l'exposition involontaire au réseau des instances Amazon EC2. Pour plus d'informations, consultez le [Guide de l'utilisateur Amazon Inspector](#).
- Utilisez AWS Security Hub des contrôles pour surveiller vos ressources Amazon EC2 par rapport aux meilleures pratiques de sécurité et aux normes de sécurité. Pour plus d'informations sur l'utilisation de Security Hub, veuillez consulter la rubrique [Contrôles Amazon Elastic Compute Cloud](#) dans le Guide de l'utilisateur AWS Security Hub .

Stockage

- Maîtrisez les implications du type de périphérique racine pour la persistance, la sauvegarde et la récupération des données. Pour plus d'informations, veuillez consulter [Stockage pour le périphérique racine](#).
- Utilisez des volumes Amazon EBS distincts pour le système d'exploitation et vos données. Assurez-vous que le volume avec vos données persiste après la fin de l'instance. Pour plus d'informations, veuillez consulter [Conservation des données lors de la résiliation d'une instance](#).
- Utilisez le stockage d'instance disponible pour que votre instance stocke les données temporaires. Souvenez-vous que les données stockées dans un stockage d'instance sont supprimées quand vous arrêtez, mettez en veille prolongée ou résiliez votre instance. Si vous utilisez le stockage

d'instance pour le stockage de base de données, assurez-vous d'avoir un cluster avec un facteur de réplication qui garantit la tolérance aux pannes.

- Chiffrez les volumes EBS et les instantanés. Pour plus d'informations, consultez la section relative au [chiffrement Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Gestion des ressources

- Utilisez les métadonnées d'instances et les balises de ressource personnalisées pour suivre et identifier vos ressources AWS . Pour plus d'informations, consultez [Utiliser des métadonnées d'instance](#) et [Baliser vos ressources Amazon EC2](#).
- Affichez vos limites actuelles pour Amazon EC2. Prévoyez de demander les augmentations de limite avant le moment où vous en aurez besoin. Pour plus d'informations, consultez [Quotas de service Amazon EC2](#).
- Utilisez-le AWS Trusted Advisor pour inspecter votre AWS environnement, puis formuler des recommandations lorsque des opportunités se présentent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité. Pour plus d'informations, consultez [AWS Trusted Advisor](#) dans le Guide de l'utilisateur AWS Support .

Sauvegarde et restauration

- Sauvegardez régulièrement vos volumes EBS à l'aide des [instantanés Amazon EBS](#) et créez une [Amazon Machine Image \(AMI\)](#) à partir de votre instance afin d'enregistrer la configuration en tant que modèle pour lancer les futures instances. Pour plus d'informations sur AWS les services permettant de réaliser ce cas d'utilisation, consultez [AWS BackupAmazon Data Lifecycle Manager](#).
- Déployez les composants critiques de votre application à travers plusieurs zones de disponibilité et répliquez vos données de manière appropriée.
- Concevez vos applications pour gérer l'adressage IP dynamique au redémarrage de votre instance. Pour plus d'informations, veuillez consulter [Adressage IP des instances Amazon EC2](#).
- Surveillez les événements et répondez-y. Pour plus d'informations, veuillez consulter [Surveiller Amazon EC2](#).
- Vérifiez bien que vous êtes prêt à gérer le failover (basculement). Pour une solution de base, vous pouvez attacher manuellement une interface réseau ou une adresse IP Elastic à une instance de remplacement. Pour plus d'informations, veuillez consulter [Interfaces réseau Elastic](#). Pour une solution automatisée, vous pouvez utiliser Amazon EC2 Auto Scaling. Pour plus d'informations, consultez le [Amazon EC2 Auto Scaling Guide de l'utilisateur](#).

- Testez régulièrement le processus de restauration de vos instances et volumes Amazon EBS pour vous assurer que les données et les services sont restaurés correctement.

Réseaux

- Définissez la valeur time-to-live (TTL) pour vos applications sur 255, pour IPv4 et IPv6. Si vous utilisez une valeur inférieure, la durée de vie risque d'expirer pendant le transit du trafic de l'application, ce qui entraînerait des problèmes d'accessibilité pour vos instances.

Amazon Machine Images (AMI)

Une Amazon Machine Image (AMI) est une image prise en charge et maintenue fournie par AWS qui fournit les informations requises pour lancer une instance. Vous devez spécifier une AMI lorsque vous lancez une instance. Lorsque vous avez besoin de plusieurs instances configurées de manière identique, il est possible de lancer plusieurs instances à partir d'une même AMI. Lorsque vous avez besoin d'instances configurées de manière différente, vous pouvez utiliser différentes AMI pour lancer ces instances.

Une AMI comprend les éléments suivants :

- Un ou plusieurs instantanés Amazon Elastic Block Store (Amazon EBS) ou, pour les AMI, un modèle instance-store-backed pour le volume racine de l'instance (par exemple, un système d'exploitation, un serveur d'applications et des applications).
- Autorisations de lancement qui contrôlent AWS les comptes autorisés à utiliser l'AMI pour lancer des instances.
- Un mappage de périphérique de stockage en mode bloc qui spécifie les volumes à attacher à l'instance lorsqu'elle est lancée.

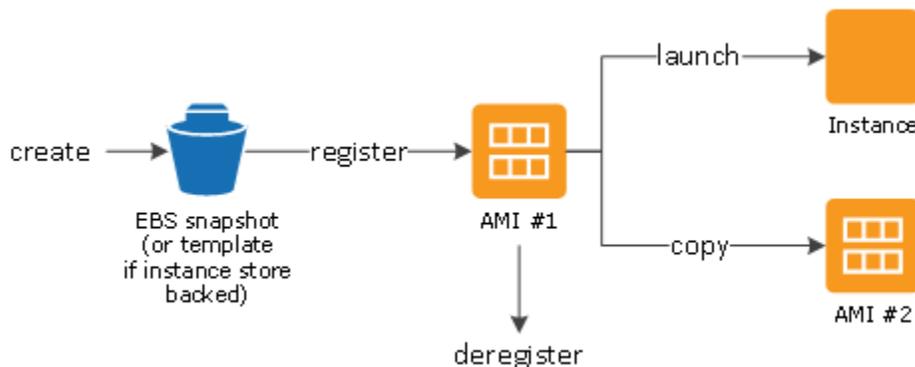
Rubriques Amazon Machine Image (AMI)

- [Utiliser une AMI](#)
- [Créer votre propre AMI](#)
- [Acheter, partager et vendre des AMI](#)
- [Annuler l'enregistrement de votre AMI](#)
- [Amazon Linux 2023 et Amazon Linux 2](#)
- [AMI Windows](#)
- [Types d'AMI](#)
- [Types de virtualisation AMI](#)
- [Modes de démarrage Amazon EC2](#)
- [Rechercher une AMI](#)
- [AMI partagées](#)
- [AMI payantes](#)

- [Cycle de vie de l'AMI](#)
- [Utiliser le chiffrement avec des AMI basées sur EBS](#)
- [Surveillez les événements AMI à l'aide d'Amazon EventBridge](#)
- [Comprendre les informations de facturation d'AMI](#)
- [Quotas d'AMI](#)

Utiliser une AMI

Le diagramme suivant résume le cycle de vie de l'AMI. Après avoir créé et enregistré une AMI, vous pouvez l'utiliser pour lancer de nouvelles instances. Vous pouvez également lancer des instances depuis une AMI si son propriétaire vous octroie des autorisations de lancement. Vous pouvez copier une AMI dans la même AWS région ou dans différentes AWS régions. Lorsque vous n'avez plus besoin d'une AMI, vous pouvez annuler son inscription.



Vous pouvez rechercher une AMI répondant aux critères de votre instance. Vous pouvez rechercher des AMI fournies par AWS ou par la communauté. Pour plus d'informations, consultez [Types d'AMI](#) et [Rechercher une AMI](#).

Une fois que vous avez lancé une instance à partir d'une AMI, vous pouvez vous y connecter. Lorsque vous êtes connecté à une instance, vous pouvez l'utiliser comme vous le feriez avec n'importe quel autre serveur. Pour plus d'informations sur le lancement, la connexion et l'utilisation de votre instance, consultez [Mise en route avec Amazon EC2](#).

Créer votre propre AMI

Vous pouvez lancer une instance à partir d'une AMI existante, personnaliser l'instance (par exemple, [installer un logiciel](#) sur l'instance), puis enregistrer cette configuration mise à jour en tant qu'AMI

personnalisée. Les instances lancées à partir de cette nouvelle AMI incluront les personnalisations apportées lors de sa création.

Le périphérique de stockage racine de l'instance détermine le processus à suivre pour créer une AMI. Le volume racine d'une instance est soit un volume Amazon Elastic Block Store (Amazon EBS), soit un volume de stockage d'instances. Pour plus d'informations sur les volumes du périphérique racine, consultez [Volume racine de l'instance Amazon EC2](#).

- Pour créer une AMI basée sur Amazon EBS, consultez [Création d'une AMI basée sur Amazon EBS](#).
- Pour créer une AMI basée sur le stockage d'instances, consultez [Créer une AMI Linux basée sur le stockage d'instance](#).

Pour faciliter le classement et la gestion de vos AMI, vous pouvez leur attribuer des balises personnalisées. Pour plus d'informations, consultez [Baliser vos ressources Amazon EC2](#).

Acheter, partager et vendre des AMI

Après avoir créé une AMI, vous pouvez la garder privée afin que vous soyez le seul à pouvoir l'utiliser, ou vous pouvez la partager avec une liste de AWS comptes spécifiée. Vous pouvez également rendre votre AMI personnalisée publique afin que la communauté puisse l'utiliser. La création d'une AMI sûre, sécurisée et utilisable à des fins d'utilisation publique est un processus relativement simple, à condition que vous respectiez quelques consignes simples. Pour plus d'informations sur la création et l'utilisation d'AMI partagées, consultez [AMI partagées](#).

Vous pouvez acheter des AMI auprès d'un tiers, notamment si elle est fournie avec des contrats de service proposés par des organisations telles que Red Hat. Vous pouvez également créer une AMI et la vendre à d'autres utilisateurs Amazon EC2. Pour plus d'informations sur la vente ou l'achat d'AMI, consultez [AMI payantes](#).

Annuler l'enregistrement de votre AMI

Vous pouvez annuler l'inscription de votre AMI lorsque vous avez terminé de l'utiliser. Après cette opération, l'AMI ne peut plus être utilisée pour lancer de nouvelles instances. Les instances existantes lancées à partir de l'AMI ne sont pas affectées. Pour plus d'informations, consultez [Désenregistrer \(supprimer\) une AMI](#).

Amazon Linux 2023 et Amazon Linux 2

La dernière version d'Amazon Linux, AL2023, est optimisée pour Amazon EC2 et est fournie sans frais supplémentaires aux utilisateurs d'Amazon EC2. Les fonctionnalités d'AL2023 incluent une cadence de publication prévisible, des mises à jour fréquentes et un support à long terme.

Pour plus d'informations sur les fonctionnalités d'AL2023 et le lancement d'une AMI AL2023, consultez :

- [Fonctionnalités d'AL2023](#)
- [Commencer avec AL2023](#)

Amazon Linux 2 (AL2) fournit un environnement d'exécution stable, sécurisé et performant pour les applications exécutées sur Amazon EC2. Pour plus d'informations sur Amazon Linux 2, consultez [Amazon Linux 2 sur Amazon EC2](#) dans le guide de l'utilisateur Amazon Linux 2.

Note

L'AMI Amazon Linux a atteint sa limite end-of-life le 31 décembre 2023 et ne recevra aucune mise à jour de sécurité ni aucune correction de bogue à compter du 1er janvier 2024. Pour plus d'informations sur l'AMI Amazon Linux end-of-life et le support de maintenance, consultez le billet de blog [Update on Amazon Linux AMI end-of-life](#). Nous vous recommandons de mettre à niveau les applications vers AL2023, qui inclut un support à long terme jusqu'en 2028.

AMI Windows

AWS fournit un ensemble d'AMI accessibles au public qui contiennent des configurations logicielles spécifiques à la plate-forme Windows. Vous pouvez commencer rapidement à créer et à déployer vos applications avec Amazon EC2 à l'aide de ces AMI. Commencez par choisir l'AMI qui répond à vos besoins, puis lancez une instance à l'aide de cette AMI. Vous récupérez le mot de passe du compte administrateur, puis vous vous connectez à l'instance à l'aide de Remote Desktop Connection, comme vous le feriez avec n'importe quel autre serveur Windows. Pour plus d'informations sur les AMI AWS Windows, consultez la [référence des AMI AWS Windows](#).

Lorsque vous lancez une instance à partir d'une AMI Windows, le périphérique racine de l'instance Windows est un volume Amazon Elastic Block Store (Amazon EBS). Les AMI Windows ne prennent pas en charge le stockage d'instance pour le périphérique racine.

Les AMI Windows configurées pour un lancement plus rapide avec EC2 Fast Launch sont préconfigurées, à l'aide de snapshots pour lancer les instances jusqu'à 65 % plus rapidement. Pour en savoir plus sur EC2 Fast Launch, consultez [Utilisez EC2 Fast Launch pour vos instances Windows](#).

Note

Microsoft ne prend plus en charge les versions de Windows Server antérieures à Windows Server 2016. Nous vous recommandons de lancer les nouvelles instances EC2 avec une version prise en charge de Windows Server. Si vous avez des instances EC2 existantes qui utilisent une version non prise en charge de Windows Server, nous vous recommandons de mettre à niveau ces instances vers une version prise en charge de Windows Server. Pour plus d'informations, consultez [Mettre à niveau une instance Amazon EC2 Windows vers une nouvelle version de Windows Server](#).

Types d'AMI

Vous pouvez sélectionner une AMI en fonction des caractéristiques suivantes :

- Région (consultez [Régions et zones](#))
- Système d'exploitation
- Architecture (32 bits ou 64 bits)
- [Autorisations de lancement](#)
- [Stockage pour le périphérique racine](#)

Autorisations de lancement

Le propriétaire d'une AMI détermine sa disponibilité en spécifiant les autorisations de lancement. Les autorisations de lancement sont réparties en plusieurs catégories.

Autorisation de lancement	Description
public	Le propriétaire accorde des autorisations de lancement à tous les AWS comptes.
explicite	Le propriétaire accorde des autorisations de lancement à des AWS comptes, organisations ou unités organisationnelles (UO) spécifiques.
implicite	Le propriétaire a des autorisations de lancement implicites pour une AMI.

Amazon et la communauté Amazon EC2 proposent un large éventail d'AMI publiques. Pour plus d'informations, consultez [AMI partagées](#). Les développeurs peuvent faire payer leurs AMI. Pour plus d'informations, consultez [AMI payantes](#).

Stockage pour le périphérique racine

Toutes les AMI sont réparties en deux catégories : basées sur Amazon EBS ou basées sur le stockage d'instances.

- AMI d'Amazon EBS : le périphérique racine d'une instance lancée à partir de l'AMI est un volume Amazon Elastic Block Store (Amazon EBS) créé à partir d'un instantané Amazon EBS. Compatible avec les AMI Linux et Windows.
- AMI Amazon basée sur le stockage d'instances : le périphérique racine d'une instance lancée à partir de l'AMI est un volume de stockage d'instances créé à partir d'un modèle stocké dans Amazon S3. Pris en charge uniquement pour les AMI Linux. Les AMI Windows ne prennent pas en charge le stockage d'instances pour le périphérique racine.

Pour plus d'informations, consultez [Volume racine de l'instance Amazon EC2](#).

Le tableau suivant résume les différences importantes lors de l'utilisation des deux types d'AMI.

Caractéristiques	AMI basée sur des volumes Amazon EBS	AMI basée sur le stockage d'instances Amazon
	Généralement inférieur à 1 minute	

Caractéristiques	AMI basée sur des volumes Amazon EBS	AMI basée sur le stockage d'instances Amazon
Temps de démarrage pour une instance		Généralement inférieur à 5 minutes
Limite de taille d'un périphérique racine	64 TiB**	10 Gio
volume du périphérique racine	Volume EBS	Volume de stockage d'instances
Persistance des données	Par défaut, le volume racine est supprimé lorsque l'instance est arrêtée.* Par défaut, les données des autres volumes EBS sont conservées après la mise hors service de l'instance.	Les données des volumes de stockage d'instances sont conservées uniquement pendant la durée de vie de l'instance.
Modifications	Le type d'instance, le noyau, le disque RAM et les données utilisateur peuvent être modifiés pendant que l'instance est arrêtée.	Les attributs de l'instance restent les mêmes pendant la durée de vie de l'instance.
Frais	Les éléments suivants vous sont facturés : utilisation de l'instance, utilisation du volume EBS et stockage de votre AMI sous forme d'instantané EBS.	L'utilisation de l'instance et le stockage de l'AMI dans Amazon S3 vous sont facturés.
Création de l'AMI/bundle	Utilise une seule commande/un seul appel	Requiert l'installation et l'utilisation des outils AMI

Caractéristiques	AMI basée sur des volumes Amazon EBS	AMI basée sur le stockage d'instances Amazon
État d'arrêt	Peut être à l'état arrêté. Même lorsque l'instance est arrêtée et ne s'exécute pas, le volume racine est conservé dans Amazon EBS	Ne peut pas être dans un état arrêté, les instances sont en cours d'exécution ou hors service

* Par défaut, les volumes racines EBS ont l'indicateur `DeleteOnTermination` défini sur `true`. Pour plus d'informations sur la modification de cet indicateur afin que le volume soit conservé après la mise hors service, consultez [Modifier le volume racine pour qu'il persiste](#).

** Pris en charge avec `io2` EBS Block Express uniquement. Pour plus d'informations, consultez la section [Volumes SSD Block Express provisionnés par IOPS](#) dans le guide de l'utilisateur Amazon EBS.

Déterminer le type de périphérique racine de votre AMI

Pour déterminer le type de périphérique racine d'une AMI à l'aide de la console

- Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
- Dans le panneau de navigation, choisissez AMI, puis sélectionnez l'AMI.
- Vérifiez la valeur de Root Device Type (Type de périphérique racine) sous l'onglet Details (Détails) comme suit :
 - `ebs` : il s'agit d'une AMI basée sur EBS.
 - `instance store` : il s'agit d'une AMI basée sur le stockage d'instances.

Pour déterminer le type de périphérique racine d'une AMI à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur ces interfaces ligne de commande, consultez [Accès à Amazon EC2](#).

- [describe-images](#) (AWS CLI)
- [Get-EC2Image](#) (AWS Tools for Windows PowerShell)

État d'arrêt

Vous pouvez arrêter une instance qui possède un volume EBS comme périphérique racine, mais vous ne pouvez pas arrêter une instance qui possède un volume de stockage d'instances comme périphérique racine.

Lorsque vous choisissez d'arrêter une instance, vous interrompez son exécution (son statut passe de `running` à `stopping`, puis à `stopped`). Une instance arrêtée est conservée sur Amazon EBS, ce qui lui permet d'être redémarrée. L'arrêt est différent de la mise hors service dans la mesure où vous ne pouvez pas redémarrer une instance qui a été mise hors service. Étant donné que les instances avec un volume de stockage d'instances comme périphérique racine ne peuvent pas être arrêtées, elles sont soit en cours d'exécution, soit hors service. Pour plus d'informations sur ce qui se produit et ce que vous pouvez faire lors de l'arrêt d'une instance, consultez [Arrêtez et démarrez les instances Amazon EC2](#).

Persistance et stockage de données par défaut

Les instances qui utilisent un volume de stockage d'instances comme périphérique racine ont un stockage d'instances disponible automatiquement (le volume racine contient la partition racine et vous pouvez stocker des données supplémentaires). Vous pouvez ajouter un stockage permanent à votre instance en attachant un ou plusieurs volumes EBS. Toute donnée présente sur un volume de stockage d'instances est effacée lorsque l'instance échoue ou qu'elle est mise hors service. Pour plus d'informations, consultez [Volume du stockage d'instances et durée de vie des données](#).

Les instances qui utilisent Amazon EBS comme périphérique racine sont automatiquement attachées à un volume EBS. Le volume apparaît dans votre liste de volumes comme tous les autres. Avec la plupart des types d'instance, les instances qui ont un volume EBS comme périphérique racine n'ont aucun volume de stockage d'instances par défaut. Vous pouvez ajouter des volumes de stockage d'instances ou des volumes EBS supplémentaires à l'aide d'un mappage de périphérique de stockage en mode bloc. Pour plus d'informations, consultez [Mappages de périphériques de stockage en mode bloc](#).

Temps de démarrage

Les instances lancées depuis une AMI basée sur Amazon EBS se lancent plus rapidement que celles lancées depuis une AMI basée sur le stockage d'instances. Lorsque vous lancez une instance depuis une AMI basée sur le stockage d'instances, toutes les parties doivent être extraites d'Amazon S3 avant que l'instance soit disponible. Dans le cadre d'une AMI basée sur Amazon EBS, seules

les parties nécessaires au démarrage de l'instance doivent être extraites de l'instantané avant que l'instance soit disponible. Toutefois, les performances d'une instance qui utilise un volume EBS pour son périphérique racine sont plus lentes pendant un bref moment, tandis que les parties restantes sont extraites de l'instantané et chargées dans le volume. Lorsque vous arrêtez et redémarrez l'instance, celle-ci est lancée rapidement dans la mesure où l'état est stocké dans un volume EBS.

Création de l'AMI

Pour créer des AMI Linux basées sur le stockage d'instances, vous devez créer une AMI à partir de votre instance sur l'instance elle-même à l'aide des outils AMI Amazon EC2. Notez que les AMI Windows ne prennent pas en charge le stockage d'instance pour le périphérique racine.

La création de l'AMI est nettement plus simple pour les AMI basées sur Amazon EBS. L'action d'API `CreateImage` crée votre AMI basée sur Amazon EBS et l'inscrit. Il contient également un bouton AWS Management Console qui vous permet de créer une AMI à partir d'une instance en cours d'exécution. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).

Facturation

Pour les AMI basées sur le stockage d'instances, le stockage de l'AMI dans Amazon S3 et l'utilisation de l'instance vous sont facturés. Avec les AMI basées sur Amazon EBS, l'utilisation de l'instance, le stockage de volume EBS et son utilisation, ainsi que le stockage de votre AMI comme instantané EBS vous sont facturés.

Avec les AMI basées sur le stockage d'instances Amazon EC2, chaque fois que vous personnalisez une AMI et que vous en créez une nouvelle, toutes les parties sont stockées dans Amazon S3 pour chaque AMI. Par conséquent, c'est la taille complète de chaque AMI personnalisée qui est stockée. Avec les AMI basées sur Amazon EBS, chaque fois que vous personnalisez une AMI et que vous en créez une nouvelle, seules les modifications sont stockées. L'espace de stockage nécessaire pour les AMI personnalisées qui suivent la première est donc bien plus réduit, ce qui entraîne des frais de stockage des AMI moins élevés.

Lorsqu'une instance ayant un volume EBS comme périphérique racine est arrêtée, l'utilisation de l'instance n'est pas facturée, mais le stockage du volume l'est. Dès que vous démarrez votre instance, nous facturons au minimum une minute pour l'utilisation. Après une minute, seules les secondes utilisées vous sont facturées. Si, par exemple, vous exécutez une instance pendant 20 secondes, puis que vous l'arrêtez, nous vous facturons une minute complète. Si vous exécutez une instance pendant 3 minutes et 40 secondes, nous vous facturons exactement 3 minutes et 40 secondes d'utilisation. Chaque seconde, avec un minimum d'une minute, pendant laquelle votre

instance s'exécute vous est facturée, même si l'instance demeure inactive et que vous ne vous y connectez pas.

Types de virtualisation AMI

Les Amazon Machine Images utilisent l'un des deux types de virtualisation : virtualisation paravirtuelle ou virtualisation HVM. Les principales différences entre les AMI de virtualisation paravirtuelle ou virtualisation HVM résident dans leur façon de démarrer et leur capacité à tirer parti des extensions matérielles spéciales (UC, réseau et stockage) pour obtenir une meilleure performance. Les AMI Windows sont des AMI HVM.

Pour obtenir les meilleures performances, nous vous recommandons d'utiliser les types d'instance de la génération actuelle et les AMI HVM quand vous lancez vos instances. Pour plus d'informations sur les types d'instance de la génération actuelle, consultez [Types d'instance Amazon EC2](#). Si vous utilisez des types d'instance de la génération précédente et souhaitez effectuer une mise à niveau, consultez [Procédures de mise à niveau](#) et [Modifier le type d'instance](#).

Le tableau suivant compare les AMI HVM et PV.

	HVM	Virtualisation paravirtuelle
Description	Les AMI HVM sont présentées avec un ensemble entièrement virtualisé de matériel et démarrent en exécutant l'enregistrement d'amorçage maître du périphérique de stockage en mode bloc racine de votre image. Ce type de virtualisation permet d'exécuter un système d'exploitation directement par-dessus une machine virtuelle sans aucune modification, comme si elle était exécutée sur le matériel bare-metal. Le système hôte Amazon EC2 émule une partie	Les AMIs de virtualisation paravirtuelle démarrent avec un chargeur de démarrage spécial appelé PV-GRUB qui lance le cycle de démarrage, puis charge en chaîne le noyau spécifié dans le fichier menu.lst sur votre image. Les invités de virtualisation paravirtuelle peuvent s'exécuter sur du matériel hôte qui ne prend pas explicitement en charge la virtualisation. Traditionnellement, les invités de virtualisation paravirtuelle avaient de

	HVM	Virtualisation paravirtuelle
	ou tout le matériel sous-jacent qui est présenté à l'invité.	meilleures performances que les invités HVM. A cause des améliorations de la virtualisation HVM et de la disponibilité des pilotes de virtualisation paravirtuelle pour les AMI HVM, ce n'est plus le cas. Pour plus d'informations sur PV-GRUB et son utilisation dans Amazon EC2, consultez la section Noyaux fournis par l'utilisateur.

	HVM	Virtualisation paravirtuelle
Prise en charge des extensions matérielles	<p>Oui. Contrairement aux invités PV, les invités HVM peuvent profiter des extensions matérielles qui offrent un accès rapide au matériel sous-jacent sur le système hôte. Pour plus d'informations sur les extensions de virtualisation du processeur disponibles dans Amazon EC2, consultez la section Technologie de virtualisation Intel sur le site Web d'Intel.</p> <p>Les AMI HVM sont obligatoires pour tirer parti de la mise en réseau améliorée et du traitement GPU. Afin de passer les instructions sur le réseau spécialisé et les appareils GPU, le système d'exploitation doit pouvoir avoir accès à la plate-forme matérielle initiale. La virtualisation HVM donne cet accès. Pour plus d'informations, consultez Mise en réseau améliorée sur Amazon EC2.</p>	<p>Non, ils ne peuvent pas tirer parti des extensions matérielles spéciales telles que la mise en réseau améliorée ou le traitement GPU.</p>

	HVM	Virtualisation paravirtuelle
Types d'instance pris en charge	Tous les types d'instance de la génération actuelle prennent en charge les AMI HVM.	Les types d'instance de la génération précédente prennent en charge les AMI PV suivantes : C1, C3, M1, M3, M2 et T1. Les types d'instance de la génération actuelle ne prennent en charge les AMI de virtualisation paravirtuelle.
Régions prises en charge	Toutes les régions prennent en charge les instances HVM.	Asie-Pacifique (Tokyo), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), Europe (Francfort), Europe (Irlande), Amérique du Sud (São Paulo), US East (N. Virginia), USA Ouest (Californie du Nord) et USA Ouest (Oregon)
Comment trouver	Vérifiez que le type de virtualisation de l'AMI est défini sur <code>hvm</code> à l'aide de la console ou de la commande describe-images . Pour plus d'informations, consultez Rechercher une AMI .	Vérifiez que le type de virtualisation de l'AMI est défini sur <code>paravirtual</code> à l'aide de la console ou de la commande describe-images . Pour plus d'informations, consultez Rechercher une AMI .

Virtualisation paravirtuelle sur HVM

Les invités paravirtuels avaient traditionnellement de meilleures performances en ce qui concerne les opérations de stockage et les opérations réseau que les invités HVM, car ils pouvaient tirer parti de pilotes spéciaux pour les I/O qui évitaient la surcharge du réseau et du disque matériel en émulation. Les invités HVM devaient quant à eux appliquer ces instructions à du matériel émulé. Maintenant, les pilotes de virtualisation paravirtuelle sont disponibles pour les invités HVM, donc les systèmes d'exploitation qui ne peuvent pas être utilisés dans un environnement paravirtualisé peuvent encore

connaître des avantages en termes de performance en ce qui concerne le stockage et l'I/O du réseau en les utilisant. Avec ces pilotes de virtualisation paravirtuelle sur HVM, les invités HVM peuvent obtenir une performance similaire, ou meilleure, que les invités paravirtuels.

Modes de démarrage Amazon EC2

Lorsqu'un ordinateur démarre, le premier logiciel qu'il exécute est responsable d'initialiser la plateforme et de fournir une interface permettant au système d'exploitation d'effectuer des opérations spécifiques à la plateforme.

Dans Amazon EC2, deux variantes du logiciel de mode de démarrage sont prises en charge : l'interface UEFI (Unified Extensible Firmware Interface) et le BIOS hérité.

Paramètres de mode de démarrage possible sur une AMI

Une AMI peut avoir l'une des valeurs de paramètre de mode de démarrage suivantes : `uefi`, `legacy-bios` ou `uefi-preferred`. Le paramètre de mode d'amorçage de l'AMI est facultatif. Les instances lancées à partir des AMI sans paramètre de mode de démarrage utilisent la valeur de mode de démarrage par défaut du type d'instance.

Objectif du paramètre de mode d'amorçage de l'AMI

Le paramètre de mode de démarrage de l'AMI signale à Amazon EC2 le mode de démarrage à utiliser lors du lancement d'une instance. Lorsque le paramètre de mode de démarrage est défini sur `uefi`, EC2 tente de lancer l'instance sur l'UEFI. Si le système d'exploitation n'est pas configuré pour prendre en charge l'UEFI, le lancement de l'instance échoue.

Paramètre de mode de démarrage d'UEFI préféré

Vous pouvez créer des AMI qui prennent en charge à la fois l'UEFI et le BIOS hérité à l'aide du paramètre de mode de démarrage `uefi-preferred`. Lorsque le paramètre de mode de démarrage est défini sur `uefi-preferred` et si le type d'instance prend en charge l'UEFI, l'instance est lancée sur l'UEFI. Si le type d'instance ne prend pas en charge l'UEFI, l'instance est lancée sur le BIOS hérité.

Warning

Certaines fonctionnalités, comme UEFI Secure Boot, ne sont disponibles que sur les instances qui démarrent sur l'UEFI. Lorsque vous utilisez le paramètre de mode de démarrage d'AMI `uefi-preferred` avec un type d'instance qui ne prend pas en charge

l'UEFI, l'instance est lancée en tant que BIOS hérité et la fonctionnalité dépendante de l'UEFI est désactivée. Si vous vous appuyez sur la disponibilité d'une fonctionnalité dépendante de l'UEFI, définissez le paramètre du mode de démarrage de votre AMI sur `uefi`.

Modes de démarrage par défaut pour les types d'instance

- Types d'instances Graviton : UEFI
- Types d'instances Intel et AMD : BIOS hérité

Types d'instances Intel et AMD pouvant s'exécuter sur l'UEFI

[Most Intel and AMD instance types](#) peut être exécuter à la fois sur l'UEFI et sur le BIOS Legacy. Pour utiliser l'UEFI, vous devez sélectionner une AMI dont le paramètre de mode de démarrage est défini sur `uefi` ou `uefi-preferred`, et le système d'exploitation contenu dans l'AMI doit être configuré pour prendre en charge l'UEFI.

Rubriques Mode de démarrage

- [Lancer une instance](#)
- [Déterminer le paramètre de mode de démarrage d'une AMI](#)
- [Déterminer les modes de démarrage pris en charge d'un type d'instance](#)
- [Déterminer le mode de démarrage d'une instance](#)
- [Déterminer le mode de démarrage du système d'exploitation](#)
- [Définir le mode de démarrage d'une AMI](#)
- [Variables UEFI](#)
- [UEFI Secure Boot](#)

Lancer une instance

Vous pouvez lancer une instance en mode de démarrage de UEFI ou du BIOS hérité.

Rubriques

- [Limites](#)
- [Considérations](#)
- [Conditions requises pour lancer une instance sur l'UEFI](#)

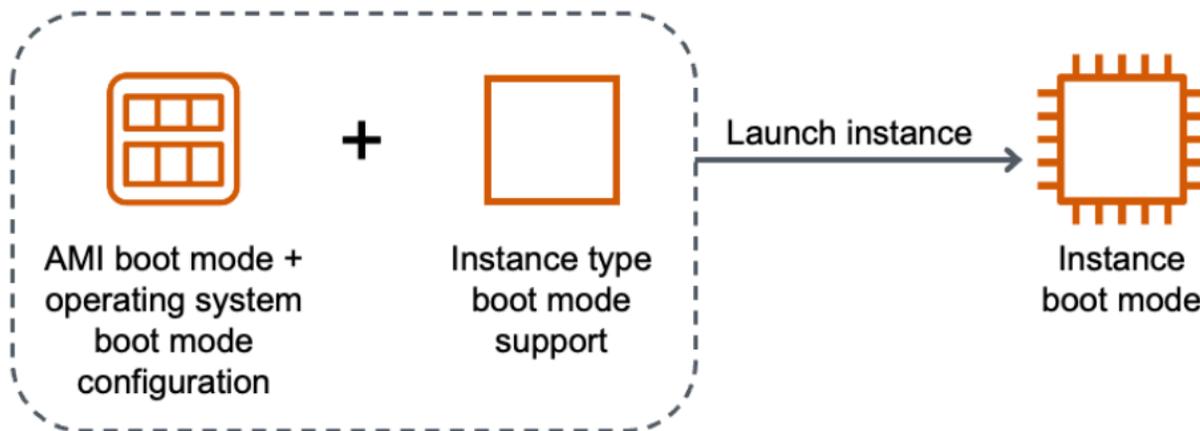
Limites

Le démarrage UEFI n'est pas pris en charge par les Local Zones, zones Wavelength ou avec AWS Outposts.

Considérations

Tenez compte des éléments suivants lors du lancement d'une instance :

- Le mode de démarrage de l'instance est déterminé par la configuration de l'AMI, le système d'exploitation qu'elle contient et le type d'instance, comme illustré par l'image suivante :



Le tableau suivant montre que le mode de démarrage d'une instance (indiqué par la colonne Mode de démarrage de l'instance résultante) est déterminé par une combinaison du paramètre de mode de démarrage de l'AMI (colonne 1), de la configuration du mode de démarrage du système d'exploitation contenu dans l'AMI (colonne 2) et de la prise en charge du mode de démarrage du type d'instance (colonne 3).

Paramètre de mode de démarrage AMI	Configuration du mode de démarrage du système d'exploitation	Prise en charge du mode de démarrage du type d'instance	Mode de démarrage de l'instance résultante
UEFI	UEFI	UEFI	UEFI
BIOS hérité	BIOS hérité	BIOS hérité	BIOS hérité

Paramètre de mode de démarrage AMI	Configuration du mode de démarrage du système d'exploitation	Prise en charge du mode de démarrage du type d'instance	Mode de démarrage de l'instance résultante
UEFI préférée	UEFI	UEFI	UEFI
UEFI préférée	UEFI	UEFI et BIOS hérité	UEFI
UEFI préférée	BIOS hérité	BIOS hérité	BIOS hérité
UEFI préférée	BIOS hérité	UEFI et BIOS hérité	BIOS hérité
Aucun mode de démarrage spécifié – ARM	UEFI	UEFI	UEFI
Aucun mode de démarrage spécifié – x86	BIOS hérité	UEFI et BIOS hérité	BIOS hérité

- Modes de démarrage par défaut :
 - Types d'instances Graviton : UEFI
 - Types d'instances Intel et AMD : BIOS hérité
- Intel et les types d'instances AMD prenant en charge l'interface UEFI, en plus du BIOS hérité :
 - Toutes les instances basées sur le système AWS Nitro, à l'exception des instances bare metal, DL1, G4ad, P4, u-3tb1, u-6tb1, u-9tb1, u-12tb1, u-18tb1, u-24tb1 et VT1

Pour consulter les types d'instance disponibles qui prennent en charge la mise en veille prolongée dans une Région spécifique

Les types d'instance disponibles varient selon l' Région AWS. Pour consulter les types d'instance disponibles qui prennent en charge la mise en veille prolongée dans une Région, utilisez la commande [describe-instance-types](#) avec le paramètre `--region`. Si vous omettez le paramètre `--region`, votre [région par défaut](#) est utilisée dans la demande. Incluez le paramètre `--filters` pour

étendre les résultats aux types d'instance qui prennent en charge UEFI et le paramètre `--query` pour étendre la sortie à la valeur de `InstanceType`.

Utilisez la commande correspondant à votre système d'exploitation.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c5.12xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
  Where-Object {$_.SupportedBootModes -Contains "uefi"} | `
  Sort-Object InstanceType | `
  Format-Table InstanceType -GroupBy CurrentGeneration
```

```
CurrentGeneration: False
```

```
InstanceType
```

```
-----
```

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
```

```
CurrentGeneration: True
```

```
InstanceType
```

```
-----
```

```
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
...
```

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
Name=processor-info.supported-architecture,Values=x86_64 --query "InstanceTypes[*].
[InstanceType]" --output text | sort
```

```
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
c5.large
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
  Where-Object {
    $_.SupportedBootModes -Contains "uefi" -and `
    $_.ProcessorInfo.SupportedArchitectures -eq "x86_64"
  } | `
  Sort-Object InstanceType | `
  Format-Table InstanceType -GroupBy CurrentGeneration
```

```
CurrentGeneration: True
```

```
InstanceType
-----
c5.12xlarge
c5.18xlarge
c5.24xlarge
```

```
c5.2xlarge
c5.4xlarge
...
```

Pour consulter les types d'instance disponibles qui prennent en charge UEFI Secure Boot (démarrage sécurisé UEFI) et les variables non volatiles persistantes dans une Région spécifique

Actuellement, les instances matériel nu ne prennent pas en charge UEFI Secure Boot et les variables non volatiles. Utilisez la commande [describe-instance-types](#) comme décrit dans l'exemple précédent, mais filtrez les instances matériel nu en incluant le filtre `Name=bare-metal,Values=false`. Pour plus d'informations sur UEFI Secure Boot, consultez [UEFI Secure Boot](#).

Utilisez la commande correspondant à votre système d'exploitation.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
Name=bare-metal,Values=false --query "InstanceTypes[*].[InstanceType]" --output
text | sort
```

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False
    } | `
    Sort-Object InstanceType | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
    @{Name="SupportedArchitectures";
    Expression={$_.ProcessorInfo.SupportedArchitectures}}
```

InstanceType	SupportedBootModes	BareMetal	SupportedArchitectures
a1.2xlarge	{uefi}	False	arm64
a1.4xlarge	{uefi}	False	arm64
a1.large	{uefi}	False	arm64
a1.medium	{uefi}	False	arm64
a1.xlarge	{uefi}	False	arm64
c5.12xlarge	{legacy-bios, uefi}	False	x86_64
c5.18xlarge	{legacy-bios, uefi}	False	x86_64

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi Name=bare-metal,Values=false Name=processor-info.supported-architecture,Values=x86_64 --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

```
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
  Where-Object { `
    $_.SupportedBootModes -Contains "uefi" -and `
    $_.BareMetal -eq $False -and `
    $_.ProcessorInfo.SupportedArchitectures -eq "x86_64" `
  } | `
  Sort-Object InstanceType | `
  Format-Table InstanceType, SupportedBootModes, BareMetal, `
  @{Name="SupportedArchitectures"; `
  Expression={$_.ProcessorInfo.SupportedArchitectures}}
```

InstanceType	SupportedBootModes	BareMetal	SupportedArchitectures
c5.12xlarge	{legacy-bios, uefi}	False	x86_64

c5.18xlarge	{legacy-bios, uefi}	False	x86_64
c5.24xlarge	{legacy-bios, uefi}	False	x86_64
c5.2xlarge	{legacy-bios, uefi}	False	x86_64
c5.4xlarge	{legacy-bios, uefi}	False	x86_64
c5.9xlarge	{legacy-bios, uefi}	False	x86_64

Conditions requises pour lancer une instance sur l'UEFI

Pour lancer une instance en mode de démarrage UEFI, vous devez sélectionner un type d'instance prenant en charge l'UEFI et configurer l'AMI et le système d'exploitation pour l'UEFI, comme suit :

Type d'instance

Lors du lancement d'une instance, vous devez sélectionner un type d'instance prenant en charge UEFI. Pour plus d'informations, consultez [Déterminer les modes de démarrage pris en charge d'un type d'instance](#).

AMI

Lors du lancement d'une instance, vous devez sélectionner une AMI configurée pour UEFI. L'AMI doit être configurée comme suit :

- Système d'exploitation : le système d'exploitation contenu dans l'AMI doit être configuré pour utiliser UEFI sinon, le lancement de l'instance échouera. Pour plus d'informations, consultez [Déterminer le mode de démarrage du système d'exploitation](#).
- Paramètre du mode de démarrage de l'AMI : le paramètre de mode de démarrage de l'AMI doit être défini sur `uefi` ou `uefi-preferred`. Pour plus d'informations, consultez [Déterminer le paramètre de mode de démarrage d'une AMI](#).

Linux : fournit AWS uniquement des AMI Linux configurées pour prendre en charge l'UEFI pour les types d'instances basés sur Graviton. Pour utiliser Linux sur d'autres types d'instances UEFI, vous devez [configurer l'AMI, importer l'AMI](#) via [VM Import/Export ou](#) importer l'AMI via [CloudEndure](#)

Windows : les AMI Windows suivantes prennent en charge l'UEFI :

- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Core-Base

- TPM-Windows_Server-2016-English-Full-Base
- TPM-Windows_Server-2016-English-Core-Base

Déterminer le paramètre de mode de démarrage d'une AMI

Le paramètre de mode d'amorçage de l'AMI est facultatif. Une AMI peut avoir l'une des valeurs de paramètre de mode de démarrage suivantes : `uefi`, `legacy-bios` ou `uefi-preferred`.

Certaines AMI n'ont pas de paramètre de mode de démarrage. Lorsqu'une AMI n'a pas de paramètre de mode de démarrage, les instances lancées à partir de l'AMI utilisent la valeur par défaut du type d'instance, qui est `uefi` sur Graviton et `legacy-bios` sur les types d'instance Intel et AMD.

Console

Pour déterminer le paramètre de mode de démarrage d'une AMI (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez AMI, puis sélectionnez l'AMI.
3. Vérifiez le champ Mode de démarrage.
 - Une valeur `uefi` indique que l'AMI prend en charge UEFI.
 - Une valeur `uefi-preferred` indique que l'AMI prend en charge l'UEFI et le BIOS hérité.
 - S'il n'existe aucune valeur, les instances lancées à partir de l'AMI utilisent la valeur par défaut du type d'instance.

Pour déterminer le paramètre de mode de démarrage d'une AMI lors du lancement d'une instance (console)

Lors du lancement d'une instance à l'aide de l'assistant de lancement d'instance, à l'étape de sélection d'une AMI, vérifiez le champ Mode de démarrage. Pour plus d'informations, consultez [Images d'applications et de systèmes d'exploitation \(Amazon Machine Image\)](#).

AWS CLI

Pour déterminer le paramètre de mode de démarrage d'une AMI (AWS CLI)

Utilisez l'opération [describe-images](#) pour déterminer le mode de démarrage d'une AMI.

```
aws ec2 describe-images --region us-east-1 --image-id ami-0abcdef1234567890
```

```
{
  "Images": [
    {
      ...
    ],
    "EnaSupport": true,
    "Hypervisor": "xen",
    "ImageOwnerAlias": "amazon",
    "Name": "UEFI_Boot_Mode_Enabled-Windows_Server-2016-English-Full-
Base-2020.09.30",
    "RootDeviceName": "/dev/sda1",
    "RootDeviceType": "ebs",
    "SriovNetSupport": "simple",
    "VirtualizationType": "hvm",
    "BootMode":
  "uefi"
  }
]
```

Dans la sortie, le champ `BootMode` indique le mode de démarrage de l'AMI. Une valeur de `uefi` indique que l'AMI prend en charge UEFI. Une valeur de `uefi-preferred` indique que l'AMI prend en charge l'UEFI et le BIOS hérité. S'il n'existe aucune valeur, les instances lancées à partir de l'AMI utilisent la valeur par défaut du type d'instance.

PowerShell

Pour déterminer le paramètre de mode de démarrage d'une AMI (Outils pour PowerShell)

Utilisez la l'applet de commande [Get-EC2Image](#) pour déterminer le mode de démarrage d'une AMI.

```
PS C:\> Get-EC2Image -Region us-east-1 -ImageId ami-0abcdef1234567890 | Format-List
Name, BootMode, TpmSupport

Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
BootMode   : uefi
TpmSupport : v2.0
```

Dans la sortie, le champ `BootMode` indique le mode de démarrage de l'AMI. Une valeur de `uefi` indique que l'AMI prend en charge UEFI. Une valeur de `uefi-preferred` indique que l'AMI

prend en charge l'UEFI et le BIOS hérité. S'il n'existe aucune valeur, les instances lancées à partir de l'AMI utilisent la valeur par défaut du type d'instance.

Déterminer les modes de démarrage pris en charge d'un type d'instance

Vous pouvez utiliser le AWS CLI ou les outils PowerShell pour déterminer les modes de démarrage pris en charge pour un type d'instance.

Pour déterminer les modes de démarrage pris en charge d'un type d'instance

Vous pouvez utiliser les méthodes suivantes pour déterminer les modes de démarrage pris en charge d'un type d'instance.

AWS CLI

Vous pouvez utiliser la commande [describe-instance-types](#) pour déterminer les modes de démarrage pris en charge d'un type d'instance. En incluant le paramètre `--query`, vous pouvez filtrer la sortie. Dans cet exemple, la sortie est filtrée pour ne renvoyer que les modes de démarrage pris en charge.

L'exemple suivant montre que `m5.2xlarge` prend en charge les modes de démarrage de l'UEFI et du BIOS hérité.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types m5.2xlarge --query "InstanceTypes[*].SupportedBootModes"
```

Sortie attendue :

```
[
  [
    "legacy-bios",
    "uefi"
  ]
]
```

L'exemple suivant montre que `t2.xlarge` ne prend en charge que le BIOS hérité.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types t2.xlarge --query "InstanceTypes[*].SupportedBootModes"
```

Sortie attendue :

```
[
  [
    "legacy-bios"
  ]
]
```

PowerShell

Vous pouvez utiliser l'applet de commande [Get-EC2InstanceType](#) (Tools for PowerShell) pour déterminer les modes de démarrage pris en charge par un type d'instance.

L'exemple suivant montre que `m5.2xlarge` prend en charge les modes de démarrage de l'UEFI et du BIOS hérité.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType m5.2xlarge | Format-List
InstanceType, SupportedBootModes
```

Sortie attendue :

```
InstanceType      : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

L'exemple suivant montre que `t2.xlarge` ne prend en charge que le BIOS hérité.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType t2.xlarge | Format-List
InstanceType, SupportedBootModes
```

Sortie attendue :

```
InstanceType      : t2.xlarge
SupportedBootModes : {legacy-bios}
```

Déterminer le mode de démarrage d'une instance

Le mode de démarrage d'une instance est affiché dans le champ Mode de démarrage de la console Amazon EC2, et par le paramètre `currentInstanceBootMode` de l'AWS CLI.

Lorsqu'une instance est lancée, la valeur de son paramètre de mode de démarrage est déterminée par la valeur du paramètre de mode de démarrage de l'AMI utilisée pour la lancer, comme suit :

- Une AMI avec un paramètre de mode de démarrage défini sur `uefi` crée une instance avec un paramètre `currentInstanceBootMode` de `uefi`.
- Une AMI avec un paramètre de mode de démarrage défini sur `legacy-bios` crée une instance avec un paramètre `currentInstanceBootMode` de `legacy-bios`.
- Une AMI dont le paramètre de mode de démarrage est `uefi-preferred` crée une instance avec un paramètre `currentInstanceBootMode` de `uefi` si le type d'instance prend en charge l'UEFI ; sinon, elle crée une instance avec un paramètre `currentInstanceBootMode` de `legacy-bios`.
- Une AMI sans valeur de paramètre de mode de démarrage crée une instance avec une valeur de paramètre de `currentInstanceBootMode` qui dépend du fait que l'architecture de l'AMI est ARM ou x86 et du mode de démarrage pris en charge du type d'instance. Le mode de démarrage par défaut est `uefi` sur les types d'instance Graviton et `legacy-bios` sur les types d'instance Intel et AMD.

Console

Pour déterminer le mode de démarrage d'une instance (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Sous l'onglet Détails, vérifiez le champ Mode de démarrage.

AWS CLI

Pour déterminer le mode de démarrage d'une instance (AWS CLI)

Utilisez la commande [describe-instances](#) pour déterminer le mode de démarrage d'une instance. Vous pouvez également déterminer le mode de démarrage de l'AMI qui a été utilisée pour créer l'instance.

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0

{
  "Reservations": [
    {
```

```
"Groups": [],
"Instances": [
  {
    "AmiLaunchIndex": 0,
    "ImageId": "ami-0e2063e7f6dc3bee8",
    "InstanceId": "i-1234567890abcdef0",
    "InstanceType": "m5.2xlarge",
    ...
  },
  "BootMode": "uefi",
  "CurrentInstanceBootMode": "uefi"
}
],
"OwnerId": "1234567890",
"ReservationId": "r-1234567890abcdef0"
}
]
```

PowerShell

Pour déterminer le mode de démarrage d'une instance (Outils pour PowerShell)

Utilisez l'applet de commande [Get-EC2Image](#) pour déterminer le mode de démarrage d'une instance. Vous pouvez également déterminer le mode de démarrage de l'AMI qui a été utilisée pour créer l'instance.

[Get-EC2Image](#) (AWS Tools for Windows PowerShell)

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
CurrentInstanceBootMode, InstanceType, ImageId
```

```
BootMode           : uefi
CurrentInstanceBootMode : uefi
InstanceType       : c5a.large
ImageId            : ami-0265446f88eb4021b
```

Dans la sortie, les paramètres suivants décrivent le mode de démarrage :

- **BootMode** : le mode de démarrage de l'AMI qui a été utilisée pour créer l'instance.
- **CurrentInstanceBootMode** : le mode de démarrage utilisé pour démarrer l'instance au lancement ou au démarrage.

Déterminer le mode de démarrage du système d'exploitation

Le mode de démarrage de l'AMI guide Amazon EC2 vers le mode de démarrage à utiliser pour démarrer une instance. Pour savoir si le système d'exploitation de votre instance est configuré pour UEFI, vous devez vous connecter à votre instance via SSH (instances Linux) ou RDP (instances Windows).

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Linux

Pour déterminer le mode de démarrage du système d'exploitation de l'instance

1. [Connectez-vous à votre instance Linux à l'aide de SSH.](#)
2. Pour afficher le mode de démarrage du système d'exploitation, essayez l'une des méthodes suivantes :
 - Exécutez la commande suivante.

```
[ec2-user ~]$ sudo /usr/sbin/efibootmgr
```

Sortie attendue d'une instance démarrée en mode de démarrage UEFI

```
BootCurrent: 0001
Timeout: 0 seconds
BootOrder: 0000,0001
Boot0000* UiApp
Boot0001* UEFI Amazon Elastic Block Store vol-xyz
```

- Exécutez la commande suivante pour vérifier l'existence du répertoire `/sys/firmware/efi`. Ce répertoire n'existe que si l'instance démarre à l'aide de l'UEFI. Si le répertoire n'existe pas, la commande renvoie Legacy BIOS Boot Detected.

```
[ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo "Legacy BIOS Boot Detected"
```

Sortie attendue d'une instance démarrée en mode de démarrage UEFI

```
UEFI Boot Detected
```

Sortie attendue d'une instance démarrée en mode de démarrage BIOS hérité

```
Legacy BIOS Boot Detected
```

- Exécutez la commande suivante pour vérifier qu'EFI apparaît dans la sortie dmesg.

```
[ec2-user ~]$ dmesg | grep -i "EFI"
```

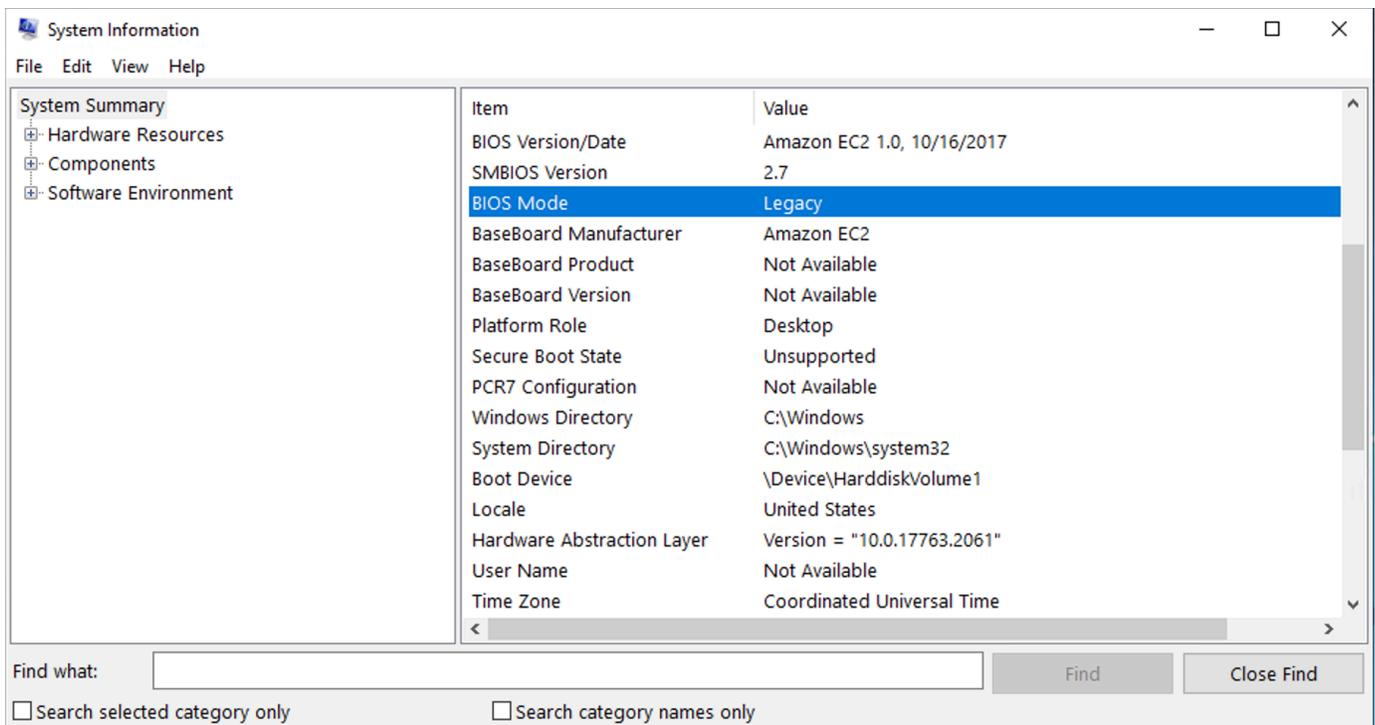
Sortie attendue d'une instance démarrée en mode de démarrage UEFI

```
[ 0.000000] efi: Getting EFI parameters from FDT:  
[ 0.000000] efi: EFI v2.70 by EDK II
```

Windows

Pour déterminer le mode de démarrage du système d'exploitation de l'instance

1. [Connectez-vous à votre instance Windows à l'aide de RDP.](#)
2. Accédez à Informations système et vérifiez la ligne Mode BIOS.



Définir le mode de démarrage d'une AMI

Lorsque vous créez une AMI à l'aide de la commande [register-image](#), vous pouvez définir le mode de démarrage de l'AMI sur `uefi`, `legacy-bios` ou `uefi-preferred`.

Lorsque le mode de démarrage de l'AMI est défini sur `uefi-preferred`, l'instance démarre comme suit :

- Pour les types d'instance qui prennent en charge à la fois l'UEFI et le BIOS hérité (par exemple, `m5.large`), l'instance démarre à l'aide de l'UEFI.
- Pour les types d'instance qui prennent en charge uniquement le BIOS hérité (par exemple, `m4.large`), l'instance démarre à l'aide du BIOS hérité.

Note

Si vous définissez le mode de démarrage de l'AMI sur `uefi-preferred`, le système d'exploitation doit prendre en charge le démarrage de l'UEFI et du BIOS hérité.

Actuellement, vous ne pouvez pas utiliser la commande [register-image](#) pour créer une AMI prenant en charge à la fois [NitroTPM](#) et l'UEFI préférée.

Warning

Certaines fonctionnalités, comme UEFI Secure Boot, ne sont disponibles que sur les instances qui démarrent sur l'UEFI. Lorsque vous utilisez le paramètre de mode de démarrage d'AMI `uefi-preferred` avec un type d'instance qui ne prend pas en charge l'UEFI, l'instance est lancée en tant que BIOS hérité et la fonctionnalité dépendante de l'UEFI est désactivée. Si vous vous appuyez sur la disponibilité d'une fonctionnalité dépendante de l'UEFI, définissez le paramètre du mode de démarrage de votre AMI sur `uefi`.

Pour convertir une instance existante basée sur le BIOS hérité en UEFI, ou une instance existante basée sur UEFI en BIOS hérité, vous devez effectuer plusieurs étapes : tout d'abord, modifiez le volume et le système d'exploitation de l'instance pour prendre en charge le mode de démarrage sélectionné. Créez ensuite un instantané du volume. Enfin, utilisez [register-image](#) pour créer l'AMI à l'aide de l'instantané.

Vous ne pouvez pas définir le mode de démarrage d'une AMI à l'aide de la commande [create-image](#). Avec [create-image](#), l'AMI hérite du mode de démarrage de l'instance EC2 utilisée pour créer l'AMI. Par exemple, si vous créez une AMI à partir d'une instance EC2 exécutée sur un BIOS hérité, le mode de démarrage de l'AMI sera configuré en tant que `legacy-bios`. Si vous créez une AMI à partir d'une instance EC2 lancée avec une AMI dont le mode de démarrage est défini sur `uefi-preferred`, son mode de démarrage sera également défini sur `uefi-preferred`.

 Warning

La définition du paramètre de mode de démarrage de l'AMI ne configure pas automatiquement le système d'exploitation pour le mode de démarrage spécifié. Avant de procéder à ces étapes, vous devez d'abord apporter des modifications appropriées au volume et au système d'exploitation de l'instance pour prendre en charge le démarrage via le mode de démarrage sélectionné. Dans le cas contraire, l'AMI résultante ne sera pas utilisable. Par exemple, si vous convertissez une instance Windows basée sur le BIOS Legacy en UEFI, vous pouvez utiliser l'outil [MBR2GPT](#) de Microsoft pour convertir le disque système de MBR en GPT. Les modifications requises sont spécifiques au système d'exploitation. Pour plus d'informations, consultez le manuel de votre système d'exploitation.

Pour définir le mode de démarrage d'une AMI (AWS CLI)

1. Apporter des modifications appropriées au volume et au système d'exploitation de l'instance pour prendre en charge le démarrage via le mode de démarrage sélectionné. Les modifications requises sont spécifiques au système d'exploitation. Pour plus d'informations, consultez le manuel de votre système d'exploitation.

 Note

Si vous n'effectuez pas cette étape, l'AMI ne sera pas utilisable.

2. Pour trouver l'ID de volume de l'instance, utilisez la commande [describe-instances](#). Vous allez créer un instantané de ce volume à l'étape suivante.

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0
```

Sortie attendue

```
...
    "BlockDeviceMappings": [
      {
        "DeviceName": "/dev/sda1",
        "Ebs": {
          "AttachTime": "",
          "DeleteOnTermination": true,
          "Status": "attached",
          "VolumeId": "vol-1234567890abcdef0"
        }
      }
    ]
  }
  ...
```

3. Pour créer un instantané du volume, utilisez la commande [create-snapshot](#). Utilisez l'ID de volume de l'étape précédente.

```
aws ec2 create-snapshot --region us-east-1 --volume-id vol-1234567890abcdef0 --
description "add text"
```

Sortie attendue

```
{
  "Description": "add text",
  "Encrypted": false,
  "OwnerId": "123",
  "Progress": "",
  "SnapshotId": "snap-01234567890abcdef",
  "StartTime": "",
  "State": "pending",
  "VolumeId": "vol-1234567890abcdef0",
  "VolumeSize": 30,
  "Tags": []
}
```

4. Notez l'ID d'instantané dans la sortie de l'étape précédente.
5. Attendez que la création de l'instantané soit complétée avant de passer à l'étape suivante. Pour interroger l'état de l'instantané, utilisez la commande [describe-snapshots](#).

```
aws ec2 describe-snapshots --region us-east-1 --snapshot-ids snap-01234567890abcdef
```

Exemple de sortie

```
{
  "Snapshots": [
    {
      "Description": "This is my snapshot",
      "Encrypted": false,
      "VolumeId": "vol-049df61146c4d7901",
      "State": "completed",
      "VolumeSize": 8,
      "StartTime": "2019-02-28T21:28:32.000Z",
      "Progress": "100%",
      "OwnerId": "012345678910",
      "SnapshotId": "snap-01234567890abcdef",
      ...
    }
  ]
}
```

6. Pour créer une AMI, utilisez la commande [register-image](#). Utilisez l'ID d'instantané que vous avez noté à l'étape précédente.
 - Pour définir le mode de démarrage sur l'UEFI, ajoutez le paramètre `--boot-mode` à la commande et spécifiez `uefi` comme valeur.

```
aws ec2 register-image \
  --region us-east-1 \
  --description "add description" \
  --name "add name" \
  --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
  --architecture x86_64 \
  --root-device-name /dev/sda1 \
  --virtualization-type hvm \
  --ena-support \
  --boot-mode uefi
```

- Pour définir le mode de démarrage sur `uefi-preferred`, ajoutez le paramètre `--boot-mode` à la commande et spécifiez `uefi-preferred` comme valeur.

```
aws ec2 register-image \
  --region us-east-1 \
  --description "add description" \
  --name "add name" \
```

```
--block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
--architecture x86_64 \
--root-device-name /dev/sda1 \
--virtualization-type hvm \
--ena-support \
--boot-mode uefi-preferred
```

Sortie attendue

```
{
  "ImageId": "ami-new_ami_123"
}
```

7. Pour vérifier que l'AMI nouvellement créée possède le mode de démarrage spécifié à l'étape précédente, utilisez la commande [describe-images](#).

```
aws ec2 describe-images --region us-east-1 --image-id ami-new_ami_123
```

Sortie attendue

```
{
  "Images": [
    {
      "Architecture": "x86_64",
      "CreationDate": "2021-01-06T14:31:04.000Z",
      "ImageId": "ami-new_ami_123",
      "ImageLocation": "",
      ...
      "BootMode": "uefi"
    }
  ]
}
```

8. Lancez une nouvelle instance à l'aide de l'AMI nouvellement créée.

Si le mode de démarrage de l'AMI est `uefi` ou `legacy-bios`, les instances créées à partir de cette AMI auront le même mode de démarrage. Si le mode de démarrage AMI est `uefi-preferred`, l'instance démarrera à l'aide de l'UEFI si le type d'instance prend en charge l'UEFI.

Dans le cas contraire, elle démarrera à l'aide du BIOS hérité. Pour plus d'informations, consultez [Considérations](#).

9. Pour vérifier que la nouvelle instance possède le mode de démarrage attendu, utilisez la commande [describe-instances](#).

Variables UEFI

Lorsque vous lancez une instance pour laquelle le mode de démarrage est défini sur UEFI, un magasin clé-valeur pour les variables est créé. Le magasin peut être utilisé par UEFI et le système d'exploitation d'instances pour stocker des variables UEFI.

Les variables UEFI sont utilisées par le chargeur de démarrage et le système d'exploitation pour configurer le démarrage précoce du système. Ils permettent au système d'exploitation de gérer certains paramètres du processus de démarrage, tels que l'ordre de démarrage ou la gestion des clés de UEFI Secure Boot.

Warning

Toute personne pouvant se connecter à l'instance (et potentiellement à tout logiciel exécuté sur l'instance), ou toute personne autorisée à utiliser l'[GetInstanceUefiData](#) API sur l'instance, peut lire les variables. Vous ne devez jamais stocker de données sensibles, telles que des mots de passe ou des informations personnelles identifiables, dans le magasin de variables UEFI.

Persistence des variables UEFI

- Pour les instances lancées le 10 mai 2022 ou avant, les variables UEFI sont effacées au redémarrage ou à l'arrêt.
- Pour les instances lancées le 11 mai 2022 ou après, les variables UEFI marquées comme non volatiles sont conservées au redémarrage et à l'arrêt/démarrage.
- Les instances matériel nu ne préservent pas les variables non volatiles UEFI dans les opérations d'arrêt/démarrage de l'instance.

UEFI Secure Boot

UEFI Secure Boot s'appuie sur le processus de démarrage sécurisé de longue date d'Amazon EC2 et fournit des fonctionnalités défense-in-depth supplémentaires qui aident les clients à protéger leurs logiciels contre les menaces persistantes après les redémarrages. Il garantit que l'instance démarre uniquement le logiciel signé avec des clés de chiffrement. Les clés sont stockées dans la base de données de clés du [Magasin de variables non volatiles UEFI](#). UEFI Secure Boot empêche la modification non autorisée du flux de démarrage de l'instance.

Rubriques

- [Comment fonctionne UEFI Secure Boot](#)
- [Lancez une instance avec prise en charge de UEFI Secure Boot](#)
- [Vérifiez si une instance est activée pour UEFI Secure Boot](#)
- [Créer une AMI Linux pour prendre en charge UEFI Secure Boot](#)
- [Comment le blob AWS binaire est créé](#)

Comment fonctionne UEFI Secure Boot

UEFI Secure Boot est une fonction spécifiée dans UEFI, qui permet de vérifier l'état de la chaîne de démarrage. Elle est conçue pour garantir que seuls les binaires UEFI vérifiés cryptographiquement sont exécutés après l'auto-initialisation du microprogramme. Ces binaires incluent les pilotes UEFI et le chargeur de démarrage principal, ainsi que des composants chargés en série.

UEFI Secure Boot spécifie quatre bases de données clés, qui sont utilisées dans une chaîne de confiance. Les bases de données sont stockées dans le magasin de variables UEFI.

La chaîne de confiance est la suivante :

Base de données de clés de plateforme (PK, Platform Key)

La base de données PK est la source de la confiance. Elle contient une clé PK publique unique utilisée dans la chaîne de confiance pour mettre à jour la base de données KEK (Key Exchange Key).

Pour modifier la base de données PK, vous devez disposer de la clé privée PK pour signer une demande de mise à jour. Cela inclut la suppression de la base de données PK en écrivant une clé PK vide.

Base de données de clés d'échange de clés (KEK)

La base de données KEK est une liste de clés KEK publiques utilisées dans la chaîne de confiance pour mettre à jour les bases de données de signature (db) et de liste d'exclusion (dbx).

Pour modifier la base de données publique KEK, vous devez disposer de la clé privée PK pour signer une demande de mise à jour.

Base de données de signature (db)

La base de données est une liste de clés publiques et de hachages utilisés dans la chaîne de confiance pour valider tous les binaires de démarrage UEFI.

Pour modifier la base de données db, vous devez disposer de la clé privée PK ou de l'une des clés privées KEK pour signer une demande de mise à jour.

Base de données de liste d'exclusion de signature (dbx)

La base de données dbx est une liste de clés publiques et de hachages binaires qui ne sont pas fiables et sont utilisés dans la chaîne de confiance comme fichier de révocation.

La base de données dbx est toujours prioritaire sur toutes les autres bases de données clés.

Pour modifier la base de données dbx, vous devez disposer de la clé privée PK ou de l'une des clés privées KEK pour signer une demande de mise à jour.

Le Forum de UEFI maintient une dbx accessible au public pour de nombreux binaires et certificats connus pour être mauvais à l'adresse <https://uefi.org/revocationlistfile>.

Important

UEFI Secure Boot impose la validation des signatures sur tous les binaires UEFI. Pour permettre l'exécution d'un binaire UEFI dans UEFI Secure Boot, vous le signez avec l'une des clés privées db décrites ci-dessus.

Par défaut, UEFI Secure Boot est désactivé et le système est en mode SetupMode. Lorsque le système est en mode SetupMode, toutes les variables clés peuvent être mises à jour sans signature cryptographique. Lorsque le PK est défini, le démarrage sécurisé UEFI est activé et est quitté.
SetupMode

Lancez une instance avec prise en charge de UEFI Secure Boot

Lorsque vous [lancez une instance](#) avec les conditions préalables suivantes, l'instance validera automatiquement les binaires de démarrage UEFI par rapport à sa base de données UEFI Secure Boot. Vous pouvez également configurer UEFI Secure Boot sur une instance après le lancement.

Note

UEFI Secure Boot protège votre instance et son système d'exploitation contre les modifications du flux de démarrage. En règle générale, UEFI Secure Boot est configuré comme partie intégrante de l'AMI. Si vous créez une AMI avec des paramètres différents de ceux de l'AMI de base, tels que la modification de la `UefiData` dans l'AMI, vous pouvez désactiver UEFI Secure Boot.

Prérequis

AMI Linux

Pour lancer une instance Linux, le démarrage sécurisé UEFI doit être activé sur l'AMI Linux.

Amazon Linux prend en charge UEFI Secure Boot avec AL2023 à partir de la version 2023.1. Cependant, UEFI Secure Boot n'est pas activé dans les AMI par défaut. Pour plus d'informations, consultez [UEFI Secure Boot](#) (français non garanti) dans le Guide de l'utilisateur AL2023. Les anciennes versions des AMI Amazon Linux ne sont pas compatibles avec UEFI Secure Boot. Pour utiliser une AMI supportée, vous devez effectuer plusieurs étapes de configuration sur votre propre AMI Linux. Pour plus d'informations, consultez [Créer une AMI Linux pour prendre en charge UEFI Secure Boot](#).

AMI Windows

Pour lancer une instance Windows, le démarrage sécurisé UEFI doit être activé sur l'AMI Windows.

Les AMI Windows suivantes sont préconfigurées pour activer UEFI Secure Boot avec des clés Microsoft :

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise

- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

Actuellement, l'importation Windows avec UEFI Secure Boot à l'aide de la commande [import-image](#) n'est pas prise en charge.

Type d'instance

- Pris en charge : tous les types d'instances virtualisées prenant en charge UEFI prennent également en charge UEFI Secure Boot. Pour connaître les types d'instances prenant en charge UEFI Secure Boot, consultez [Considérations](#).
- Non pris en charge : Les types d'instance matériel nu ne prennent pas en charge UEFI Secure Boot.

Vérifiez si une instance est activée pour UEFI Secure Boot

Instances Linux

Vous pouvez utiliser l'utilitaire `mokutil` pour vérifier si une instance Linux est activée pour UEFI Secure Boot. Si `mokutil` n'est pas installé sur votre instance, vous devez l'installer. Pour les instructions d'installation d'Amazon Linux 2, consultez <https://docs.aws.amazon.com/linux/al2/ug/find-install-software.html>. Pour les autres distributions Linux, consultez leur documentation spécifique.

Pour vérifier si une instance Linux est activée pour UEFI Secure Boot

Exécutez la commande suivante en tant que `root` sur votre instance.

```
mokutil --sb-state
```

Sortie attendue :

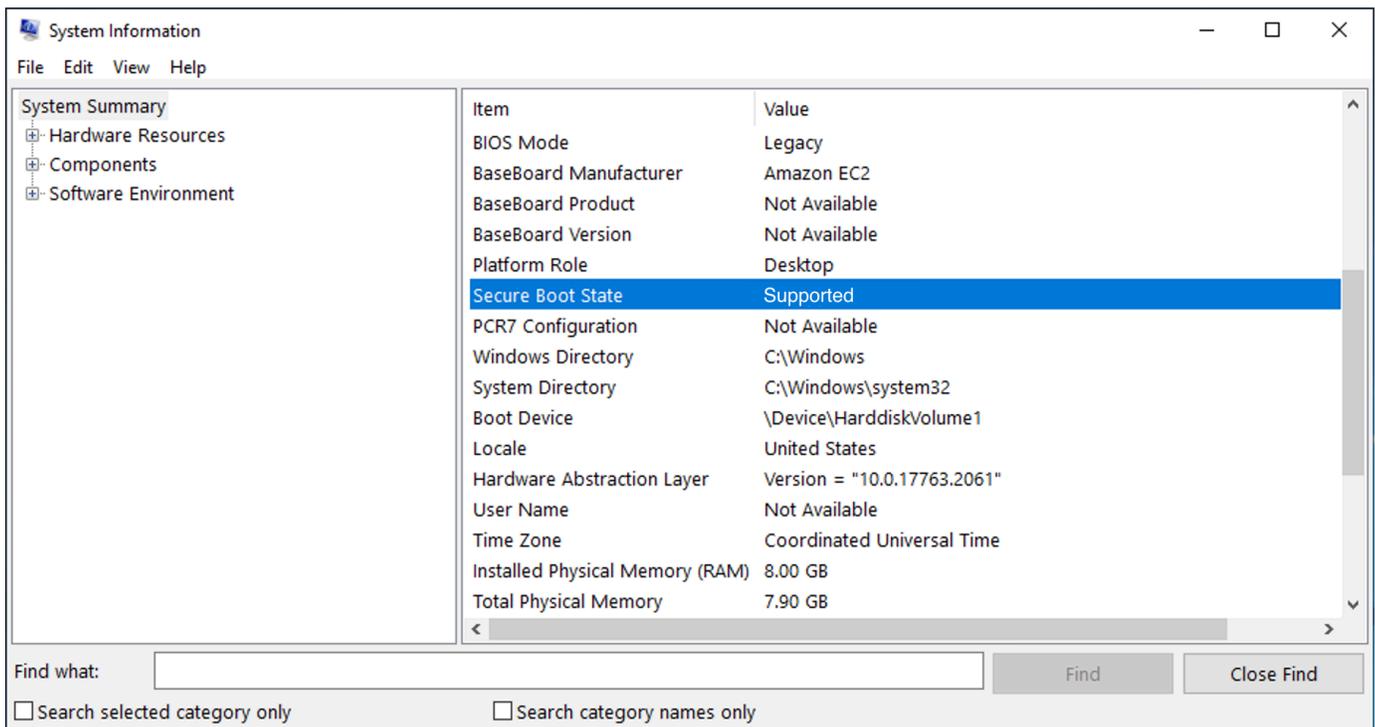
- Si UEFI Secure Boot est activé, la sortie contient `SecureBoot enabled`.

- Si UEFI Secure Boot n'est pas activé, la sortie contient `SecureBoot disabled` ou `Failed to read SecureBoot`.

instances Windows

Pour vérifier si une instance Windows est activée pour UEFI Secure Boot

1. Ouvrez l'outil `msinfo32`.
2. Vérifiez le champ `Secure Boot State` (État du démarrage sécurisé). `Supported` (Pris en charge) indique que le démarrage sécurisé de UEFI est activé.



Vous pouvez également utiliser l' PowerShell applet de commande `Windows Confirm-SecureBootUEFI` pour vérifier l'état du démarrage sécurisé. Pour plus d'informations sur l'applet de commande, consultez la section [Confirm- SecureBoot UEFI sur le site Web de](#) documentation Microsoft.

Créer une AMI Linux pour prendre en charge UEFI Secure Boot

Les procédures suivantes décrivent comment créer votre propre magasin de variables UEFI pour un démarrage sécurisé avec des clés privées personnalisées. Amazon Linux prend en charge UEFI

Secure Boot avec AL2023 à partir de la version 2023.1. Pour plus d'informations, consultez [UEFI Secure Boot](#) (français non garanti) dans le Guide de l'utilisateur AL2023.

⚠ Important

Les procédures suivantes pour créer une AMI prenant en charge UEFI Secure Boot sont destinées uniquement aux utilisateurs avancés. Vous devez posséder une connaissance suffisante de SSL et du flux de démarrage de distribution Linux pour utiliser ces procédures.

Prérequis

- Les outils suivants seront utilisés :
 - OpenSSL : <https://www.openssl.org/>
 - efivar : <https://github.com/rhboot/efivar>
 - efitools : <https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git/>
 - [commande get-instance-uefi-data](#) AWS CLI
- Votre instance Linux doit avoir été lancée avec une AMI Linux qui prend en charge le mode de démarrage UEFI et contient des données non volatiles.

Les instances nouvellement créées sans clés UEFI Secure Boot sont créées dans SetupMode, ce qui vous permet d'inscrire vos propres clés. Certaines AMI sont préconfigurées avec UEFI Secure Boot et vous ne pouvez pas modifier les clés existantes. Si vous souhaitez modifier les clés, vous devez créer une nouvelle AMI basée sur l'AMI d'origine.

Vous pouvez propager les clés dans le magasin de variables de deux manières, décrites dans les options A et B suivantes. L'option A décrit comment le faire depuis l'instance, en imitant le flux de matériel réel. L'option B décrit comment créer un blob binaire, qui est ensuite transmis en tant que fichier codé en base64 lorsque vous créez l'AMI. Pour les deux options, vous devez d'abord créer les trois paires de clés utilisées pour la chaîne de confiance.

Pour créer une AMI Linux prenant en charge UEFI Secure Boot, créez d'abord les trois paires de clés, puis complétez l'option A ou l'option B :

- [Créer la paire de clés](#)
- [Option A : ajouter des clés au magasin de variables depuis l'instance](#)
- [Option B : créer un blob binaire contenant un magasin de variables prérempli](#)

Note

Ces instructions ne peuvent être utilisées que pour créer une AMI Linux. Si vous avez besoin d'une AMI Windows, utilisez l'une des AMI Windows prises en charge. Pour plus d'informations, consultez [Lancez une instance avec prise en charge de UEFI Secure Boot](#).

Créer la paire de clés

UEFI Secure Boot repose sur les trois bases de données de clés suivantes, qui sont utilisées dans une chaîne de confiance : la clé de plateforme (PK), la clé d'échange de clés (KEK) et la base de données de signatures (db).¹

Vous créez chaque clé sur l'instance. Pour préparer les clés publiques dans un format valide pour la norme UEFI Secure Boot, vous créez un certificat pour chaque clé. DER définit le format SSL (codage binaire d'un format). Vous convertissez ensuite chaque certificat en liste de signatures UEFI, qui est le format binaire compris par UEFI Secure Boot. Enfin, vous signez chaque certificat avec la clé correspondante.

Rubriques

- [Préparez-vous à créer les paires de clés](#)
- [Paire de clés 1 : créer la clé de plateforme \(PK\)](#)
- [Paire de clés 2 : créer la clé d'échange de clés \(KEK\)](#)
- [Paire de clés 3 : créez la base de données de signatures \(db\)](#)
- [Signez l'image de démarrage \(noyau\) avec la clé privée](#)

Préparez-vous à créer les paires de clés

Avant de créer les paires de clés, créez un identifiant unique global (GUID) à utiliser lors de la génération de clés.

1. [Connectez-vous à l'instance](#).
2. Exécutez la commande suivante dans un shell.

```
uuidgen --random > GUID.txt
```

Paire de clés 1 : créer la clé de plateforme (PK)

La PK est la fondation de la confiance pour les instances UEFI Secure Boot. La PK privée est utilisée pour mettre à jour la KEK, qui peut à son tour être utilisée pour ajouter des clés autorisées à la base de données de signatures (db).

La norme X.509 est utilisée pour créer la paire de clés. Pour plus d'informations sur la norme, veuillez consulter [X.509](#) sur Wikipédia.

Pour créer la PK

1. Créez la clé. Vous devez nommer la variable PK.

```
openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -subj "/CN=Platform key/" -out PK.crt
```

Les paramètres suivants sont spécifiés :

- `-keyout PK.key` : le fichier de clé privée.
- `-days 3650` : le nombre de jours de validité du certificat.
- `-out PK.crt` : le certificat utilisé pour créer la variable UEFI.
- `CN=Platform key` : le nom commun (CN) de la clé. Vous pouvez saisir le nom de votre propre organisation à la place de *clé de plateforme*.

2. Créez le certificat.

```
openssl x509 -outform DER -in PK.crt -out PK.cer
```

3. Convertissez le certificat en liste de signatures UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
```

4. Signez la liste de signatures UEFI avec la PK privée (auto-signée).

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
```

Paire de clés 2 : créer la clé d'échange de clés (KEK)

La KEK privée est utilisée pour ajouter des clés à la base de données, qui est la liste des signatures autorisées à démarrer sur le système.

Pour créer la KEK

1. Créez la clé.

```
openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -  
subj "/CN=Key Exchange Key/" -out KEK.crt
```

2. Créez le certificat.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Convertissez le certificat en liste de signatures UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Signez la liste de signatures avec la PK privée.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Paire de clés 3 : créez la base de données de signatures (db)

La liste db contient des clés autorisées qui sont habilitées à être démarrées sur le système. Pour modifier la liste, la KEK privée est nécessaire. Les images de démarrage seront signées avec la clé privée créée au cours de cette étape.

Pour créer la db

1. Créez la clé.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -  
subj "/CN=Signature Database key/" -out db.crt
```

2. Créez le certificat.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Convertissez le certificat en liste de signatures UEFI.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Signez la liste de signatures avec la KEK privée.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Signez l'image de démarrage (noyau) avec la clé privée

Pour Ubuntu 22.04, les images suivantes nécessitent des signatures.

```
/boot/efi/EFI/ubuntu/shimx64.efi  
/boot/efi/EFI/ubuntu/mmx64.efi  
/boot/efi/EFI/ubuntu/grubx64.efi  
/boot/vmlinuz
```

Pour signer une image

Utilisez la syntaxe suivante pour signer une image.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

Note

Vous devez signer tous les nouveaux noyaux. */boot/vmlinuz* sera généralement un lien symbolique vers le dernier noyau installé.

Reportez-vous à la documentation de votre distribution pour connaître votre chaîne de démarrage et les images requises.

¹ Merci à la ArchWiki communauté pour tout le travail qu'elle a accompli. Les commandes permettant de créer le PK, de créer le KEK, de créer la base de données et de signer l'image proviennent de la section [Création de clés](#), rédigée par l'équipe de ArchWiki maintenance et/ou les ArchWiki contributeurs.

Option A : ajouter des clés au magasin de variables depuis l'instance

Une fois que vous avez créé les [trois paires de clés](#), vous pouvez vous connecter à votre instance et ajouter les clés au magasin de variables depuis l'instance en effectuant les étapes suivantes.

Étapes de l'option A :

- [Étape 1 : lancer une instance qui prend en charge le démarrage sécurisé de UEFI](#)
- [Étape 2 : configurer une instance pour prendre en charge UEFI Secure Boot](#)
- [Étape 3 : créer une AMI à partir de l'instance](#)

Étape 1 : lancer une instance qui prend en charge le démarrage sécurisé de UEFI

Lorsque vous [lancez une instance](#) avec les conditions préalables suivantes, l'instance sera alors prête à être configurée pour prendre en charge UEFI Secure Boot. Vous pouvez uniquement activer la prise en charge de UEFI Secure Boot sur une instance au lancement. Vous ne pouvez pas l'activer ultérieurement.

Prérequis

- AMI : l'AMI Linux doit prendre en charge le mode de démarrage UEFI. Pour vérifier que l'AMI prend en charge le mode de démarrage UEFI, le paramètre du mode de démarrage de l'AMI doit être uefi. Pour plus d'informations, consultez [Déterminer le paramètre de mode de démarrage d'une AMI](#).

Notez que AWS seules les AMI Linux sont configurées pour prendre en charge l'UEFI pour les types d'instances basés sur Graviton. AWS ne fournit actuellement pas d'AMI Linux x86_64 prenant en charge le mode de démarrage UEFI. Vous pouvez configurer votre propre AMI afin de prendre en charge le mode de démarrage UEFI pour toutes les architectures. Pour configurer votre propre AMI afin de prendre en charge le mode de démarrage UEFI, vous devez effectuer plusieurs étapes de configuration sur votre propre AMI Linux. Pour plus d'informations, consultez [Définir le mode de démarrage d'une AMI](#).

- Type d'instance : tous les types d'instances virtualisées prenant en charge UEFI prennent également en charge UEFI Secure Boot. Les types d'instance matériel nu ne prennent pas en charge UEFI Secure Boot. Pour connaître les types d'instances prenant en charge UEFI Secure Boot, consultez [Considérations](#).
- Lancez votre instance après la sortie d'UEFI Secure Boot. Seules les instances lancées après le 10 mai 2022 (lorsque UEFI Secure Boot a été publié) peuvent prendre en charge UEFI Secure Boot.

Une fois que vous avez lancé votre instance, vous pouvez vérifier qu'elle est prête à être configurée pour prendre en charge UEFI Secure Boot (en d'autres termes, vous pouvez passer à l'[étape 2](#)) en vérifiant si les données UEFI sont présentes. La présence de données UEFI indique que les données non volatiles sont persistantes.

Pour vérifier si votre instance est prête pour l'étape 2

Utilisez la commande [get-instance-uefi-data](#) et spécifiez l'ID de l'instance.

```
aws ec2 get-instance-uefi-data --instance-id i-0123456789example
```

L'instance est prête pour l'étape 2 si des données UEFI sont présentes dans la sortie. Si la sortie est vide, l'instance ne peut pas être configurée pour prendre en charge UEFI Secure Boot. Cela peut se produire si votre instance a été lancée avant que la prise en charge UEFI Secure Boot soit disponible. Lancez une nouvelle instance et réessayez.

Étape 2 : configurer une instance pour prendre en charge UEFI Secure Boot

Inscrivez les paires de clés dans votre magasin de variables UEFI sur l'instance

Warning

Vous devez signer vos images de démarrage après avoir inscrit les clés, sinon vous ne pourrez pas démarrer votre instance.

Après avoir créé les listes de signatures UEFI signées (PK, KEK et db), elles doivent être inscrites dans le microprogramme UEFI.

Écriture dans la variable PK n'est possible que si :

- Aucune PK n'est encore inscrite, ce qui est indiqué si la variable SetupMode est 1. Pour vérifier cela, utilisez la commande suivante. La sortie est soit 1, soit 0.

```
efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
```

- La nouvelle PK est signée par la clé privée de la PK existante.

Pour inscrire les clés dans votre magasin de variables UEFI

Les commandes suivantes doivent être exécutées sur l'instance.

Si cette option SetupMode est activée (la valeur est 1), les clés peuvent être inscrites en exécutant les commandes suivantes sur l'instance :

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

Pour vérifier que UEFI Secure Boot est activé

Pour vérifier que le démarrage sécurisé de UEFI est activé, suivez les étapes de la section [Vérifiez si une instance est activée pour UEFI Secure Boot](#).

Vous pouvez désormais exporter votre magasin de variables UEFI avec la commande CLI [get-instance-uefi-data](#), ou vous pouvez passer à l'étape suivante et signez vos images de démarrage pour redémarrer dans une instance compatible avec UEFI Secure Boot.

Étape 3 : créer une AMI à partir de l'instance

Pour créer une AMI à partir de l'instance, vous pouvez utiliser la console ou l'API, la CLI ou les SDK `CreateImage`. Pour des instructions sur l'utilisation de la console, consultez [Création d'une AMI basée sur Amazon EBS](#). Pour les instructions relatives à l'API, consultez [CreateImage](#).

Note

L'API `CreateImage` copie automatiquement le magasin de variables UEFI de l'instance vers l'AMI. La console utilise l'API `CreateImage`. Une fois que vous lancez des instances à l'aide de cette AMI, elles auront le même magasin de variables UEFI.

Option B : créer un blob binaire contenant un magasin de variables prérempli

Une fois que vous avez créé les [trois paires de clés](#), vous pouvez créer un blob binaire contenant un magasin de variables prérempli contenant les clés Secure Boot UEFI.

Warning

Vous devez signer vos images de démarrage avant d'inscrire les clés, sinon vous ne pourrez pas démarrer votre instance.

Étapes de l'option B :

- [Étape 1 : créer un nouveau magasin de variables ou mettre à jour un stockage existant](#)
- [Étape 2 : charger le blob binaire lors de la création d'AMI](#)

Étape 1 : créer un nouveau magasin de variables ou mettre à jour un stockage existant

Vous pouvez créer le magasin de variables hors ligne sans instance en cours d'exécution à l'aide de l'outil `python-uefivars`. L'outil peut créer un nouveau magasin de variables à partir de vos clés. Le script prend actuellement en charge le format EDK2, le AWS format et une représentation JSON qui est plus facile à modifier avec des outils de niveau supérieur.

Pour créer le magasin de variables hors ligne sans instance en cours d'exécution

1. Téléchargez l'outil en cliquant sur le lien suivant.

```
https://github.com/aws-labs/python-uefivars
```

2. Créez un nouveau magasin de variables à partir de vos clés en exécutant la commande suivante. Cela créera un blob binaire encodé en base64 dans `your_binary_blob.bin`. L'outil prend également en charge la mise à jour d'un blob binaire via le paramètre `-I`.

```
./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db db.esl --dbx dbx.esl
```

Étape 2 : charger le blob binaire lors de la création d'AMI

Utilisez [register-image](#) pour transmettre vos données de magasin de variables UEFI. Pour le paramètre `--uefi-data`, spécifiez votre blob binaire et pour le paramètre `--boot-mode`, spécifiez `uefi`.

```
aws ec2 register-image \  
  --name uefi_sb_tpm_register_image_test \  
  --uefi-data $(cat your_binary_blob.bin) \  
  --block-device-mappings "DeviceName=/dev/sda1,Ebs={SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \  
  --architecture x86_64 \  
  --root-device-name /dev/sda1 \  
  --virtualization-type hvm \  
  --ena-support \  
  --boot-mode uefi
```

```
--boot-mode uefi
```

Comment le blob AWS binaire est créé

Vous pouvez utiliser les étapes suivantes pour personnaliser les variables Secure Boot UEFI lors de la création de l'AMI. La KEK utilisée dans ces étapes est en date de septembre 2021. Si Microsoft met à jour la KEK, vous devez utiliser la KEK la plus récente.

Pour créer le AWS blob binaire

1. Créez une liste de signatures PK vide.

```
touch empty_key.crt  
cert-to-efi-sig-list empty_key.crt PK.esl
```

2. Téléchargez les certificats KEK.

```
https://go.microsoft.com/fwlink/?LinkId=321185
```

3. Enveloppez les certificats KEK dans une liste de signatures UEFI (siglist).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output  
MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Téléchargez les certificats db de Microsoft.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011\_2011-10-19.crt  
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011\_2011-06-27.crt
```

5. Générez la liste de signatures db.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output  
MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt  
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output  
MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt  
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. Téléchargez une demande de modification dbx mise à jour à partir du lien suivant.

```
https://uefi.org/revocationlistfile
```

7. La demande de modification dbx que vous avez téléchargée à l'étape précédente est déjà signée avec Microsoft KEK. Vous devez donc l'ouvrir ou la décompresser. Vous pouvez utiliser les liens suivants.

```
https://gist.github.com/out0xb2/f8e0bae94214889a89ac67fceb37f8c0
```

```
https://support.microsoft.com/en-us/topic/microsoft-guidance-for-applying-secure-boot-dbx-update-e3b9e4cb-a330-b3ba-a602-15083965d9ca
```

8. Créez un magasin de variables UEFI à l'aide du script `uefivars.py`.

```
./uefivars.py -i none -o aws -0 uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl --dbx ~/dbx-2021-April.bin
```

9. Vérifiez le blob binaire et le magasin de variables UEFI.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. Vous pouvez mettre à jour le blob en le transmettant à nouveau au même outil.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -0 uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl --dbx ~/dbx-2021-April.bin
```

Sortie attendue

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Rechercher une AMI

Une AMI inclut les composants et les applications, tels que le système d'exploitation et le type de volume racine, nécessaires au lancement d'une instance. Pour lancer une instance qui répond à vos besoins, vous devez trouver une AMI adaptée à vos besoins.

Lorsque vous sélectionnez une AMI, tenez compte des exigences suivantes que vous pourriez avoir pour les instances que vous souhaitez lancer :

- La région — Les identifiants AMI sont uniques à chaque AWS région.
- Système d'exploitation
- L'architecture : 32 bits (i386), 64 bits (x86_64) ou ARM 64 bits (arm64)
- Le type de périphérique racine : Amazon EBS ou stockage d'instances
- Le fournisseur (par exemple, Amazon Web Services)
- Les logiciels supplémentaires (par exemple, SQL Server)

Il existe différentes manières de trouver une AMI qui répond à vos besoins. Cette rubrique explique comment trouver une AMI à l'aide de la console Amazon EC2, AWS CLI AWS Tools for Windows PowerShell, et. AWS Systems Manager

Rubriques

- [Trouvez une AMI à l'aide de la console Amazon EC2](#)
- [Trouvez une AMI à l'aide du AWS CLI](#)
- [Trouvez une AMI à l'aide du AWS Tools for Windows PowerShell](#)
- [Rechercher une AMI à l'aide d'un paramètre de Systems Manager](#)
- [Trouvez les dernières AMI à l'aide de Systems Manager](#)
- [Plus d'informations sur la recherche d'AMI](#)

Trouvez une AMI à l'aide de la console Amazon EC2

Vous pouvez trouver des AMI à l'aide de la console Amazon EC2. Vous pouvez sélectionner dans la liste des AMI lorsque vous utilisez l'assistant de lancement d'instance pour lancer une instance, ou rechercher toutes les AMI disponibles à l'aide de la page Images.

Pour rechercher une AMI à l'aide de l'assistant de lancement d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement. Les ID AMI sont uniques à chaque AWS région.
3. Sur le tableau de bord de la console, sélectionnez Launch instance (Lancer une instance).
4. (Nouvelle console) Sous Application and OS Images (Amazon Machine Image) (Images d'application et de système d'exploitation [Amazon Machine Image]), choisissez Quick Start

(Démarrage rapide), sélectionnez le système d'exploitation (OS) de votre instance, puis, depuis Amazon Machine Image (AMI), choisissez l'une des AMI couramment utilisées dans la liste. Si vous ne voyez pas l'AMI que vous souhaitez utiliser, choisissez Browse more AMIs (Parcourir plus d'AMI) pour parcourir le catalogue complet des AMI. Pour plus d'informations, consultez [Images d'applications et de systèmes d'exploitation \(Amazon Machine Image\)](#).

(Ancienne console) Dans l'onglet Quick Start (Démarrage rapide), choisissez l'une des AMI couramment utilisées dans la liste. Si vous ne voyez pas l'AMI que vous souhaitez utiliser, choisissez l'onglet My AMIs (Mes AMI), AWS Marketplace ou Community AMIs (AMI de la communauté) pour afficher d'autres AMI. Pour plus d'informations, consultez [Étape 1 : Sélectionner d'une Amazon Machine Image \(AMI\)](#).

Pour rechercher une AMI à l'aide de la page AMIS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement. Les ID AMI sont uniques à chaque AWS région.
3. Dans le panneau de navigation, sélectionnez AMI.
4. (Facultatif) Utilisez les options de filtre et de recherche pour restreindre la liste des AMI affichées aux seules AMI qui correspondent à vos critères.

Par exemple, pour répertorier toutes les AMI fournies par AWS, choisissez Public images. Utilisez ensuite les options de recherche pour étendre davantage la liste des AMI affichées. Cliquez dans la barre Search (Rechercher) et, dans le menu, choisissez Owner alias (Alias du propriétaire), puis l'opérateur =, et enfin la valeur amazon. Pour rechercher des AMI correspondant à une plate-forme spécifique, par exemple Linux ou Windows, cliquez à nouveau sur la barre de recherche pour sélectionner Platform, puis l'opérateur =, puis le système d'exploitation dans la liste fournie.

5. (Facultatif) Cliquez sur l'icône Préférences pour sélectionner les attributs d'image à afficher, comme le type de périphérique racine. Vous pouvez également sélectionner une AMI dans la liste et afficher ses propriétés sous l'onglet Détails (Details).
6. Avant de sélectionner une AMI, il est important de vérifier si celle-ci est basée sur le stockage d'instances ou sur Amazon EBS et d'être conscient des effets de cette différence. Pour plus d'informations, consultez [Stockage pour le périphérique racine](#).

7. Pour lancer une instance à partir de cette AMI, sélectionnez-la et choisissez Lancer l'instance. Pour plus d'informations sur le lancement d'une instance à l'aide de la console, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#). Si vous n'êtes pas prêt à lancer l'instance maintenant, notez l'ID de l'AMI pour plus tard.

Trouvez une AMI à l'aide du AWS CLI

Vous pouvez utiliser la AWS CLI commande [describe-images](#) pour répertorier uniquement les AMI qui répondent à vos besoins. Une fois que vous avez trouvé une AMI qui correspond à vos critères, notez son ID afin de pouvoir l'utiliser pour lancer des instances. Pour plus d'informations, consultez [Lancer votre instance](#) dans le Guide de l'utilisateur AWS Command Line Interface .

La commande [describe-images](#) prend en charge les paramètres de filtrage. Par exemple, utilisez le paramètre `--owners` pour afficher les AMI publiques détenues par Amazon.

```
aws ec2 describe-images --owners amazon
```

Vous pouvez ajouter le filtre suivant à la commande précédente pour afficher uniquement les AMI Windows.

```
--filters "Name=platform,Values=windows"
```

Vous pouvez ajouter le filtre suivant à la commande précédente pour afficher uniquement les AMI basées sur Amazon EBS :

```
--filters "Name=root-device-type,Values=ebs"
```

Important

Si vous omettez le `--owners` paramètre dans la `describe-images` commande, toutes les images sont renvoyées pour lesquelles vous disposez d'autorisations de lancement, quel que soit leur propriétaire.

Trouvez une AMI à l'aide du AWS Tools for Windows PowerShell

Vous pouvez utiliser des PowerShell applets de commande pour répertorier uniquement les AMI Windows qui répondent à vos besoins. Pour obtenir des informations et des exemples, consultez la

section [Trouver une image de machine Amazon à l'aide de Windows PowerShell](#) dans le guide de AWS Tools for Windows PowerShell l'utilisateur.

Une fois que vous avez trouvé une AMI qui correspond à vos critères, notez son ID afin de pouvoir l'utiliser pour lancer des instances. Pour plus d'informations, consultez [Lancer une instance Amazon EC2 à l'aide de Windows PowerShell](#) dans le guide de l'AWS Tools for Windows PowerShell utilisateur.

Rechercher une AMI à l'aide d'un paramètre de Systems Manager

Lorsque vous lancez une instance à l'aide de l'assistant de lancement d'instance EC2 de la console Amazon EC2, vous pouvez soit sélectionner une AMI dans la liste (décrite [Trouvez une AMI à l'aide de la console Amazon EC2](#) dans), soit sélectionner AWS Systems Manager un paramètre pointant vers un ID d'AMI (décrit dans cette section). Si vous utilisez le code d'automatisation pour lancer vos instances, vous pouvez spécifier le paramètre Systems Manager au lieu de l'ID AMI.

Un paramètre Systems Manager est une paire clé-valeur définie par le client que vous pouvez créer dans le stockage de paramètres Systems Manager. Le stockage de paramètres fournit un magasin central pour externaliser les valeurs de configuration de vos applications. Pour plus d'informations, consultez [Stockage de paramètres AWS Systems Manager](#) dans le AWS Systems Manager Guide de l'utilisateur.

Lorsque vous créez un paramètre qui pointe vers un ID AMI, assurez-vous que vous spécifiez le type de données comme `aws:ec2:image`. Spécifier ce type de données garantit que lorsque le paramètre est créé ou modifié, la valeur du paramètre est validée en tant qu'ID AMI. Pour plus d'informations, consultez [Prise en charge des paramètres natifs pour les ID Amazon Machine Image](#) dans le AWS Systems Manager Guide de l'utilisateur.

Rubriques

- [Cas d'utilisation](#)
- [Autorisations](#)
- [Limites](#)
- [Lancer une instance à l'aide d'un paramètre Systems Manager](#)

Cas d'utilisation

Lorsque vous utilisez les paramètres Systems Manager pour pointer vers les ID AMI, il est plus facile pour vos utilisateurs de sélectionner l'AMI correcte lors du lancement d'instances. Les paramètres Systems Manager peuvent également simplifier la maintenance du code d'automatisation.

Plus facile pour les utilisateurs

Si vous devez lancer des instances à l'aide d'une AMI spécifique et si cette AMI est mise à jour régulièrement, nous vous recommandons de demander à vos utilisateurs de sélectionner un paramètre Systems Manager pour trouver l'AMI. En demandant à vos utilisateurs de sélectionner un paramètre Systems Manager, vous pouvez vous assurer que la dernière AMI est utilisée pour lancer des instances.

Par exemple, chaque mois dans votre organisation, vous pouvez créer une nouvelle version de votre AMI dotée des derniers correctifs du système d'exploitation et des applications. Vous devez également demander à vos utilisateurs de lancer des instances à l'aide de la dernière version de votre AMI. Pour vous assurer que vos utilisateurs utilisent la dernière version, vous pouvez créer un paramètre Systems Manager (par exemple, `golden-ami`) qui pointe vers l'ID AMI correct. Chaque fois qu'une nouvelle version de l'AMI est créée, vous mettez à jour la valeur de l'ID AMI dans le paramètre afin qu'elle pointe toujours vers la dernière AMI. Vos utilisateurs n'ont pas besoin de connaître les mises à jour périodiques de l'AMI, car ils continuent à sélectionner le même paramètre Systems Manager à chaque fois. Avec un paramètre Systems Manager pour votre AMI, il leur est plus facile de sélectionner l'AMI appropriée pour le lancement d'une instance.

Simplifier la maintenance du code d'automatisation

Si vous utilisez le code d'automatisation pour lancer vos instances, vous pouvez spécifier le paramètre Systems Manager au lieu de l'ID AMI. Si une nouvelle version de l'AMI est créée, vous pouvez modifier la valeur de l'ID AMI dans le paramètre afin qu'elle pointe vers la dernière AMI. Le code d'automatisation qui fait référence au paramètre n'a pas besoin d'être modifié chaque fois qu'une nouvelle version de l'AMI est créée. Cela simplifie la maintenance de l'automatisation et réduit les coûts de déploiement.

Note

Les instances en cours d'exécution ne sont pas affectées lorsque vous modifiez l'ID AMI vers lequel le paramètre Systems Manager pointe.

Autorisations

Si vous utilisez des paramètres Systems Manager qui pointent vers des ID d'AMI dans l'assistant de lancement d'instances, vous devez ajouter les autorisations suivantes à votre politique IAM :

- `ssm:DescribeParameters`— Autorise l'affichage et la sélection des paramètres de Systems Manager.
- `ssm:GetParameters`— Autorise à récupérer les valeurs des paramètres de Systems Manager.

Vous pouvez également restreindre l'accès à des paramètres Systems Manager spécifiques. Pour plus d'informations et des exemples de politiques IAM, consultez [Exemple : utiliser l'assistant de lancement d'instances d'EC2](#).

Limites

Les AMI et les paramètres Systems Manager sont spécifiques à la région. Pour utiliser le même nom de paramètre Systems Manager dans les régions, créez un paramètre Systems Manager dans chaque région avec le même nom (par exemple, `golden-ami`). Dans chaque région, pointez le paramètre Systems Manager sur une AMI de cette région.

Lancer une instance à l'aide d'un paramètre Systems Manager

Vous pouvez lancer une instance à l'aide de la console ou de l' AWS CLI. Au lieu de spécifier un ID d'AMI, vous pouvez spécifier un AWS Systems Manager paramètre qui pointe vers un ID d'AMI.

New console

Pour rechercher une AMI à l'aide d'un paramètre Systems Manager (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement.
3. Sur le tableau de bord de la console, sélectionnez Launch instance (Lancer une instance).
4. Sous Application and OS Images (Amazon Machine Image) (Images d'applications et de systèmes d'exploitation (Amazon Machine Image)), choisissez Browse more AMIs (Parcourir plus d'AMI).
5. Sélectionnez le bouton fléché à droite de la barre de recherche, puis choisissez Search by Systems Manager parameter (Rechercher par paramètre Systems Manager).

6. Pour Paramètre Systems Manager, sélectionnez un paramètre. L'ID AMI correspondant apparaît en dessous de Currently resolves to (Actuellement se résout en).
7. Choisissez Search (Rechercher). Les AMI correspondant à l'ID AMI apparaissent dans la liste.
8. Sélectionnez l'AMI dans la liste, puis choisissez Select (Sélectionner).

Pour plus d'informations sur le lancement d'une instance à l'aide de l'assistant de lancement d'instance, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Old console

Pour rechercher une AMI à l'aide d'un paramètre Systems Manager (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement.
3. Sur le tableau de bord de la console, sélectionnez Launch instance (Lancer une instance).
4. Choisissez Rechercher par paramètre Systems Manager (en haut à droite).
5. Pour Paramètre Systems Manager, sélectionnez un paramètre. L'ID AMI correspondant apparaît à côté de Currently resolves to (Se résout en).
6. Choisissez Search (Rechercher). Les AMI correspondant à l'ID AMI apparaissent dans la liste.
7. Sélectionnez l'AMI dans la liste, puis choisissez Select (Sélectionner).

Pour plus d'informations sur le lancement d'une instance à partir d'une AMI à l'aide de l'assistant de lancement d'instance, consultez [Étape 1 : Sélectionner d'une Amazon Machine Image \(AMI\)](#).

Pour lancer une instance à l'aide d'un AWS Systems Manager paramètre au lieu d'un ID d'AMI (AWS CLI)

L'exemple suivant utilise le paramètre Systems Manager `golden-ami` pour lancer une instance `m5.xlarge`. Le paramètre pointe vers un ID AMI.

Pour spécifier le paramètre dans la commande, utilisez la syntaxe suivante :

`resolve:ssm:/parameter-name`, où `resolve:ssm` est le préfixe standard et `parameter-name` est le nom du paramètre unique. Notez que le nom du paramètre est sensible à la casse. Les barres

obliques inverses pour le nom du paramètre ne sont nécessaires que si le paramètre fait partie d'une hiérarchie, par exemple `/amis/production/golden-ami`. Vous pouvez omettre la barre oblique inverse si le paramètre ne fait pas partie d'une hiérarchie.

Dans l'exemple, les paramètres `--count` et `--security-group` ne sont pas inclus. Pour `--count`, la valeur par défaut est 1. Si vous avez un VPC par défaut et un groupe de sécurité par défaut, ils sont utilisés.

```
aws ec2 run-instances
  --image-id resolve:ssm:/golden-ami
  --instance-type m5.xlarge
  ...
```

Pour lancer une instance à l'aide d'une version spécifique d'un AWS Systems Manager paramètre (AWS CLI)

Les paramètres Systems Manager ont la prise en charge de la version. Chaque itération d'un paramètre se voit attribuer un numéro de version unique. Vous pouvez référencer la version du paramètre comme suit : `resolve:ssm:parameter-name:version`, où `version` est le numéro de version unique. Par défaut, la dernière version du paramètre est utilisée lorsqu'aucune version n'est spécifiée.

L'exemple suivant utilise la version 2 du paramètre.

Dans l'exemple, les paramètres `--count` et `--security-group` ne sont pas inclus. Pour `--count`, le paramètre par défaut est 1. Si vous avez un VPC par défaut et un groupe de sécurité par défaut, ils sont utilisés.

```
aws ec2 run-instances
  --image-id resolve:ssm:/golden-ami:2
  --instance-type m5.xlarge
  ...
```

Pour lancer une instance à l'aide d'un paramètre public fourni par AWS

Systems Manager fournit des paramètres publics pour les AMI publiques fournies par AWS. Vous pouvez utiliser les paramètres publics lorsque vous lancez des instances afin de vous assurer que vous utilisez les dernières AMI.

Pour plus d'informations, consultez [Trouvez les dernières AMI à l'aide de Systems Manager](#).

Trouvez les dernières AMI à l'aide de Systems Manager

AWS Systems Manager fournit des paramètres publics pour les AMI publiques gérées par AWS. Vous pouvez utiliser les paramètres publics lorsque vous lancez des instances afin de vous assurer que vous utilisez les dernières AMI. Par exemple, le paramètre public `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` est disponible dans toutes les régions et pointe toujours vers la dernière version de l'AMI Amazon Linux 2023 pour l'architecture arm64 dans une région donnée.

Les paramètres publics sont disponibles à partir des chemins suivants :

- Linux : `/aws/service/ami-amazon-linux-latest`
- Windows – `/aws/service/ami-windows-latest`

Pour afficher la liste de toutes les AMI Linux ou Windows de la AWS région actuelle

Utilisez la AWS CLI commande [get-parameters-by-path](#) suivante pour afficher la liste de toutes les AMI Linux ou Windows de la région actuelle. AWS La valeur du `--path` paramètre est différente pour Linux et Windows.

Pour Linux :

```
aws ssm get-parameters-by-path \  
  --path /aws/service/ami-amazon-linux-latest \  
  --query "Parameters[].Name"
```

Pour Windows :

```
aws ssm get-parameters-by-path \  
  --path /aws/service/ami-windows-latest \  
  --query "Parameters[].Name"
```

Pour lancer une instance à l'aide d'un paramètre public

L'exemple suivant spécifie un paramètre public de Systems Manager pour l'ID d'image permettant de lancer une instance à l'aide de la dernière AMI Amazon Linux 2023.

Pour spécifier le paramètre dans la commande, utilisez la syntaxe suivante :

`resolve:ssm:public-parameter`, où `resolve:ssm` est le préfixe standard et `public-parameter` le chemin et le nom du paramètre public.

Dans l'exemple, les paramètres `--count` et `--security-group` ne sont pas inclus. Pour `--count`, la valeur par défaut est 1. Si vous avez un VPC par défaut et un groupe de sécurité par défaut, ils sont utilisés.

```
aws ec2 run-instances \  
  --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-  
  default-x86_64 \  
  --instance-type m5.xlarge \  
  --key-name MyKeyPair
```

Pour plus d'informations, veuillez consulter [Utilisation de paramètres publics](#) dans le Guide de l'utilisateur AWS Systems Manager .

Pour des exemples utilisant les paramètres de Systems Manager, consultez [Requête des derniers ID d'AMI Amazon Linux à l'aide du magasin de AWS Systems Manager paramètres](#) et [Requête de la dernière AMI Windows à l'aide du magasin de AWS Systems Manager paramètres](#).

Plus d'informations sur la recherche d'AMI

Pour trouver une AMI Amazon Linux 2023, consultez la section [AL2023 sur Amazon](#) EC2 dans le guide de l'utilisateur Amazon Linux 2023.

Pour trouver une AMI Ubuntu, consultez le [localisateur d'AMI Amazon EC2](#) sur le site Web de Canonical Ubuntu.

Pour trouver une AMI RHEL, consultez la section [Images Red Hat Enterprise Linux \(AMI\) disponibles sur Amazon Web Services \(AWS\)](#) sur le site Web de Red Hat.

AMI partagées

A shared AMI (une AMI partagée) est une AMI créée et mise à disposition par un développeur afin que d'autres développeurs puissent l'utiliser. L'une des façons les plus simples de se lancer avec Amazon EC2 est d'utiliser une AMI partagée qui possède les composants dont vous avez besoin, puis d'y ajouter du contenu personnalisé. Vous pouvez également créer vos propres AMI et les partager avec d'autres.

Vous utilisez une AMI partagée à vos propres risques. Amazon ne peut se porter garant de l'intégrité ou de la sécurité des AMI partagées par d'autres utilisateurs Amazon EC2. Dès lors, vous devez traiter les AMI partagées de la même façon que vous traitez un code étranger que vous envisageriez

de déployer dans votre propre centre de données, et prendre toutes les précautions nécessaires. Nous vous recommandons d'obtenir une AMI auprès d'une source de confiance, telle qu'un fournisseur vérifié.

Fournisseur vérifié

Dans la console Amazon EC2, les AMI publiques détenues par Amazon ou par un partenaire Amazon vérifié sont certifiées Fournisseur vérifié.

Vous pouvez également utiliser la AWS CLI commande [describe-images](#) pour identifier les AMI publiques provenant d'un fournisseur vérifié. Les images publiques détenues par Amazon ou par un propriétaire disposant d'un alias, qui est soit amazon soit aws-marketplace. Dans la sortie CLI, ces valeurs apparaissent pour ImageOwnerAlias. Les autres utilisateurs ne peuvent attribuer un alias à leurs AMI. Cela vous permet de trouver facilement des AMI provenant d'Amazon ou des partenaires vérifiés.

Pour devenir un fournisseur vérifié, vous devez vous inscrire en tant que vendeur sur le AWS Marketplace. Une fois enregistré, vous pouvez répertorier votre AMI sur la page AWS Marketplace. Pour plus d'informations, voir [Démarrer en tant que vendeur](#) et [Produits AMI](#) dans le Guide du vendeur AWS Marketplace .

Rubriques AMI partagées

- [Rechercher des AMI partagées](#)
- [Rendre une AMI publique](#)
- [Partager une AMI avec des organisations ou des unités d'organisations spécifiques](#)
- [Partager une AMI avec des comptes AWS spécifiques](#)
- [Annuler le partage d'une AMI avec votre Compte AWS](#)
- [Utiliser des signets](#)
- [Consignes pour les AMI Linux partagées](#)

Si vous recherchez des informations sur d'autres sujets

- Pour plus d'informations sur la création d'une AMI, consultez [the section called “Créer une AMI Linux basée sur le stockage d'instance”](#) ou [the section called “Création d'une AMI basée sur Amazon EBS”](#).
- Pour plus d'informations sur la création, la livraison et la maintenance de vos applications sur le AWS Marketplace, consultez la [AWS Marketplace Documentation](#) (Documentation de).

Rechercher des AMI partagées

Vous pouvez utiliser la console Amazon EC2 ou la ligne de commande pour trouver des AMI partagées.

Les AMI constituent une ressource régionale. Lorsque vous recherchez une AMI partagée (publique ou privée), vous devez la rechercher dans la même région que celle à partir de laquelle elle est partagée. Pour rendre une AMI disponible dans une autre région, copiez-la dans la région souhaitée, puis partagez-la. Pour plus d'informations, consultez [Copier une AMI](#).

Tâches

- [Rechercher une AMI partagée \(console\)](#)
- [Rechercher une AMI partagée \(AWS CLI\)](#)
- [Trouver une AMI partagée \(Outils pour Windows PowerShell\)](#)
- [Utiliser des AMI partagées](#)

Rechercher une AMI partagée (console)

Pour trouver une AMI privée partagée à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Dans le premier filtre, choisissez Images privées. Toutes les AMI qui ont été partagées avec vous sont listées. Pour affiner votre recherche, cliquez dans la barre Search (Rechercher) et utilisez les options de filtre du menu.

Pour trouver une AMI publique partagée à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Dans le premier filtre, choisissez Images publiques. Pour affiner votre recherche, cliquez dans la barre Recherche et utilisez les options de filtre du menu.

Pour trouver une AMI publique partagée par Amazon à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, sélectionnez AMI.
3. Dans le premier filtre, choisissez Images publiques.
4. Cliquez sur l'onglet Recherche puis, dans les options de menu qui s'affichent, choisissez alias du propriétaire, puis=, et ensuite amazon pour afficher uniquement les images publiques d'Amazon.

Pour trouver une AMI publique partagée par un fournisseur vérifié à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Catalogue AMI.
3. Choisissez AMI de la communauté.
4. La certification Fournisseur vérifié indique les AMI qui proviennent d'Amazon ou d'un partenaire vérifié.

Rechercher une AMI partagée (AWS CLI)

Utilisez la commande [describe-images](#) (AWS CLI) pour répertorier les AMI. Vous pouvez filtrer la liste des types d'AMI qui vous intéressent, comme le montrent les exemples suivants.

Exemple : Affichage de toutes les AMI publiques

La commande suivante liste toutes les AMI publiques, y compris les AMI publiques que vous possédez.

```
aws ec2 describe-images --executable-users all
```

Exemple : Affichage des AMI avec des autorisations de lancement explicites

La commande suivante liste toutes les AMI pour lesquelles vous disposez d'autorisations de lancement explicites. Cette liste n'inclut pas les AMI publiques que vous possédez.

```
aws ec2 describe-images --executable-users self
```

Exemple : Affichage des AMI appartenant à des fournisseurs vérifiés

La commande suivante liste toutes les AMI détenues par des fournisseurs vérifiés. Les AMI publiques détenues par des fournisseurs vérifiés (Amazon ou des partenaires vérifiés) disposent d'un propriétaire disposant d'un alias, qui apparaît en tant que amazon ou aws-marketplace dans

le champ de compte. Cela vous permet de trouver facilement des AMI provenant de fournisseurs vérifiés. Les autres utilisateurs ne peuvent attribuer un alias à leurs AMI.

```
aws ec2 describe-images \  
  --owners amazon aws-marketplace \  
  --query 'Images[*].[ImageId]' \  
  --output text
```

Exemple : Affichage des AMI appartenant à un compte

La commande suivante répertorie les AMI appartenant au Compte AWS spécifié.

```
aws ec2 describe-images --owners 123456789012
```

Exemple 1 : Limitation du nombre d'AMI affichées à l'aide d'un filtre

Pour réduire le nombre d'AMI affichées, utilisez un filtre pour lister uniquement les types d'AMI qui vous intéressent. Par exemple, utilisez le filtre suivant pour afficher uniquement les AMI basées sur EBS.

```
--filters "Name=root-device-type,Values=ebs"
```

Trouver une AMI partagée (Outils pour Windows PowerShell)

Utilisez la [Get-EC2Image](#) commande (Outils pour Windows PowerShell) pour répertorier les AMI. Vous pouvez filtrer la liste des types d'AMI qui vous intéressent, comme le montrent les exemples suivants.

Exemple : Affichage de toutes les AMI publiques

La commande suivante liste toutes les AMI publiques, y compris les AMI publiques que vous possédez.

```
PS C:\> Get-EC2Image -ExecutableUser all
```

Exemple : Affichage des AMI avec des autorisations de lancement explicites

La commande suivante liste toutes les AMI pour lesquelles vous disposez d'autorisations de lancement explicites. Cette liste n'inclut pas les AMI publiques que vous possédez.

```
PS C:\> Get-EC2Image -ExecutableUser self
```

Exemple : Affichage des AMI appartenant à des fournisseurs vérifiés

La commande suivante liste toutes les AMI détenues par des fournisseurs vérifiés. Les AMI publiques détenues par des fournisseurs vérifiés (Amazon ou des partenaires vérifiés) disposent d'un propriétaire disposant d'un alias, qui apparaît en tant que `amazon` ou `aws-marketplace` dans le champ de compte. Cela vous permet de trouver facilement des AMI provenant de fournisseurs vérifiés. Les autres utilisateurs ne peuvent attribuer un alias à leurs AMI.

```
PS C:\> Get-EC2Image -Owner amazon aws-marketplace
```

Exemple : Affichage des AMI appartenant à un compte

La commande suivante répertorie les AMI appartenant au Compte AWS spécifié.

```
PS C:\> Get-EC2Image -Owner 123456789012
```

Exemple 1 : Limitation du nombre d'AMI affichées à l'aide d'un filtre

Pour réduire le nombre d'AMI affichées, utilisez un filtre pour lister uniquement les types d'AMI qui vous intéressent. Par exemple, utilisez le filtre suivant pour afficher uniquement les AMI basées sur EBS.

```
-Filter @{ Name="root-device-type"; Values="ebs" }
```

Utiliser des AMI partagées

Avant d'utiliser une AMI partagée, suivez les étapes ci-après afin de vous assurer qu'il n'y a pas d'informations d'identification pré-installées qui permettraient un accès non désiré à votre instance par un tiers, ni de journalisation à distance préconfigurée susceptible de transmettre des données sensibles à un tiers. Consultez la documentation portant sur la distribution Linux utilisée par l'AMI pour en savoir plus sur la façon d'améliorer la sécurité du système.

Afin de vous assurer que vous ne perdiez pas accidentellement accès à votre instance, nous vous recommandons d'initier deux sessions SSH et de conserver la seconde session ouverte jusqu'à ce que vous retiriez les informations d'identification que vous ne reconnaissez pas, et que vous confirmiez que vous pouvez toujours vous connecter à votre instance à l'aide de SSH.

1. Identifiez et désactivez toute clé SSH publique non-autorisée. La seule clé dans le fichier devrait être la clé que vous avez utilisée pour lancer l'AMI. La commande suivante localise les fichiers `authorized_keys` :

```
[ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
```

2. Désactivez l'authentification basée sur mot de passe pour l'utilisateur racine. Ouvrez le fichier `sshd_config` et éditez la ligne `PermitRootLogin` de la façon suivante :

```
PermitRootLogin without-password
```

L'alternative est de désactiver la possibilité de se connecter à l'instance en tant qu'utilisateur racine :

```
PermitRootLogin No
```

Redémarrez le service `sshd`.

3. Vérifiez si d'autres utilisateurs peuvent se connecter à votre instance. Les utilisateurs disposant de privilèges de superutilisateur sont particulièrement dangereux. Supprimez ou verrouillez le mot de passe de tout compte inconnu.
4. Vérifiez s'il y a des ports ouverts que vous n'utilisez pas et des services de réseau en cours d'exécution en attente de connexions entrantes.
5. Pour empêcher la journalisation à distance préconfigurée, vous devez supprimer le fichier de configuration existant et redémarrer le service `rsyslog`. Par exemple :

```
[ec2-user ~]$ sudo rm /etc/rsyslog.conf  
[ec2-user ~]$ sudo service rsyslog restart
```

6. Vérifiez que toutes les tâches cron sont légitimes.

Si vous découvrez une AMI publique qui présente selon vous un risque de sécurité, contactez l'équipe de sécurité AWS . Pour plus d'informations, consultez le [Centre de sécuritéAWS](#).

Rendre une AMI publique

Vous pouvez rendre votre AMI accessible au public en la partageant avec tout le monde Comptes AWS.

Si vous souhaitez empêcher le partage public de vos AMI, vous pouvez activer le blocage de l'accès public pour les AMI. Cela bloque toute tentative de rendre publique une AMI, ce qui permet d'empêcher tout accès non autorisé à l'AMI et toute utilisation abusive potentielle des données de l'AMI. Notez que l'activation du blocage de l'accès public n'affecte pas vos AMI déjà accessibles au public, qui le restent.

Afin d'autoriser uniquement des comptes spécifiques à utiliser votre AMI pour lancer des instances, consultez la rubrique [Partager une AMI avec des comptes AWS spécifiques](#).

Table des matières

- [Considérations](#)
- [Partager une AMI avec tous les AWS comptes \(partager publiquement\)](#)
- [Bloquer l'accès public à vos AMI](#)

Considérations

Tenez compte des éléments suivants avant de rendre une AMI publique.

- Propriété — Pour rendre une AMI publique, vous Compte AWS devez être propriétaire de l'AMI.
- Région : les AMI constituent une ressource régionale. Lorsque vous partagez une AMI, elle est uniquement disponible dans la région à partir de laquelle vous l'avez partagée. Pour rendre une AMI disponible dans une autre région, copiez-la dans la région souhaitée puis partagez-la. Pour plus d'informations, consultez [Copier une AMI](#).
- Bloquer l'accès public : pour partager publiquement une AMI, le [blocage de l'accès public pour les AMI](#) doit être désactivé dans chaque région dans laquelle l'AMI sera partagée publiquement. Après avoir partagé publiquement l'AMI, vous pouvez réactiver le blocage de l'accès public pour les AMI afin d'empêcher tout partage public ultérieur de vos AMI.
- Certaines AMI ne peuvent pas être rendues publiques : si votre AMI inclut l'un des composants suivants, vous ne pouvez pas la rendre publique (mais vous pouvez la [partager avec des Comptes AWS spécifiques](#)) :
 - Volumes chiffrés
 - Instantanés de volumes chiffrés
 - Codes produits
- Évitez d'exposer des données sensibles : pour éviter d'exposer des données sensibles lorsque vous partagez une AMI, consultez les normes de sécurités spécifiées dans [Consignes pour les AMI Linux partagées](#) et suivez les actions recommandées.

- **Utilisation** : lorsque vous partagez une AMI, les utilisateurs peuvent uniquement lancer des instances à partir de l'AMI. Ils ne peuvent pas la supprimer, la partager ou la modifier. Toutefois, après avoir lancé une instance à l'aide de votre AMI, ils peuvent créer une AMI à partir de l'instance lancée.
- **Obsolescence automatique** – Par défaut, la date d'obsolescence de toutes les AMI publiques est fixée à deux ans à compter de la date de création de l'AMI. Vous pouvez définir la date d'obsolescence à moins de deux ans. Pour annuler la date de dépréciation ou pour la déplacer à une date ultérieure, vous devez rendre l'AMI privée en la [partageant](#) uniquement avec des personnes spécifiques. Comptes AWS
- **Supprimer les AMI obsolètes** : une fois qu'une AMI publique a atteint sa date d'obsolescence, si aucune nouvelle instance n'a été lancée depuis l'AMI pendant six mois ou plus, la propriété de partage publique est AWS finalement supprimée afin que les AMI obsolètes n'apparaissent pas dans les listes d'AMI publiques.
- **Facturation** : vous n'êtes pas facturé lorsque votre AMI est utilisée par d'autres personnes Comptes AWS pour lancer des instances. Les comptes qui lancent des instances à l'aide de l'AMI sont facturés pour les instances qu'ils lancent.

Partager une AMI avec tous les AWS comptes (partager publiquement)

Une fois qu'une AMI est rendue publique, elle est disponible dans les AMI de la communauté dans la console, auxquelles vous pouvez accéder depuis le Catalogue AMI dans le navigateur de gauche de la console EC2 ou lorsque vous lancez une instance à l'aide de la console. Notez que cela peut prendre quelques instants pour qu'une AMI s'affiche dans le champ AMI de la communauté une fois que vous l'avez rendue publique.

Console

Pour rendre une AMI publique

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Sélectionnez votre AMI dans la liste, puis choisissez Actions et Edit AMI permissions (Modifier des autorisations d'AMI).
4. Sous Disponibilité de l'AMI, choisissez Publique.
5. Sélectionnez Enregistrer les modifications.

AWS CLI

Chaque AMI possède une `launchPermission` propriété qui contrôle qui Comptes AWS, outre celle du propriétaire, est autorisée à utiliser cette AMI pour lancer des instances. En modifiant la `launchPermission` propriété d'une AMI, vous pouvez la rendre publique (ce qui accorde des autorisations de lancement à tous Comptes AWS) ou la partager uniquement avec les personnes Comptes AWS que vous spécifiez.

Vous pouvez ajouter ou supprimer des ID de compte de la liste des comptes disposant d'autorisations de lancement pour une AMI. Pour rendre l'AMI publique, spécifiez le groupe `all`. Vous pouvez spécifier à la fois des autorisations de lancement publiques et explicites.

Pour rendre une AMI publique

1. Utilisez la commande [modify-image-attribute](#) comme suit pour ajouter le groupe `all` à la liste `launchPermission` pour l'AMI spécifiée.

```
aws ec2 modify-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --launch-permission "Add=[{Group=all}]"
```

2. Pour vérifier les autorisations de lancement de l'AMI, utilisez la commande [describe-image-attribute](#).

```
aws ec2 describe-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --attribute launchPermission
```

3. (Facultatif) Pour rendre l'AMI de nouveau privée, supprimez le groupe `all` de ses autorisations de lancement. Veuillez noter que le propriétaire de l'AMI dispose toujours d'autorisations de lancement et n'est, par conséquent, pas affecté par cette commande.

```
aws ec2 modify-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --launch-permission "Remove=[{Group=all}]"
```

PowerShell

Chaque AMI possède une `launchPermission` propriété qui contrôle qui Comptes AWS, outre celle du propriétaire, est autorisée à utiliser cette AMI pour lancer des instances. En modifiant la

launchPermission propriété d'une AMI, vous pouvez la rendre publique (ce qui accorde des autorisations de lancement à tous Comptes AWS) ou la partager uniquement avec les personnes Comptes AWS que vous spécifiez.

Vous pouvez ajouter ou supprimer des ID de compte de la liste des comptes disposant d'autorisations de lancement pour une AMI. Pour rendre l'AMI publique, spécifiez le groupe all. Vous pouvez spécifier à la fois des autorisations de lancement publiques et explicites.

Pour rendre une AMI publique

1. Utilisez la commande [Edit-EC2ImageAttribute](#) comme suit pour ajouter le groupe all à la liste launchPermission pour l'AMI spécifiée.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute  
launchPermission -OperationType add -UserGroup all
```

2. Pour vérifier les autorisations de lancement d'une AMI, utilisez la commande [Get-EC2ImageAttribute](#) suivante.

```
PS C:\> Get-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute  
launchPermission
```

3. (Facultatif) Pour rendre l'AMI de nouveau privée, supprimez le groupe all de ses autorisations de lancement. Veuillez noter que le propriétaire de l'AMI dispose toujours d'autorisations de lancement et n'est, par conséquent, pas affecté par cette commande.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute  
launchPermission -OperationType remove -UserGroup all
```

Bloquer l'accès public à vos AMI

Pour empêcher le partage public de vos AMI, vous pouvez activer le blocage de l'accès public pour les AMI. Ce paramètre est activé au niveau du compte, mais vous devez l'activer Région AWS dans chaque compte pour lequel vous souhaitez empêcher le partage public de vos AMI.

Lorsque le blocage de l'accès public est activé, toute tentative de rendre publique une AMI est automatiquement bloquée. Toutefois, si vous possédez déjà des AMI publiques, elles restent accessibles au public.

Pour partager des AMI publiquement, vous devez désactiver le blocage de l'accès public. Lorsque vous avez terminé le partage, il est recommandé de réactiver le blocage de l'accès public pour empêcher tout partage public indésirable de vos AMI.

Vous pouvez limiter les autorisations IAM à un utilisateur administrateur afin qu'il soit le seul à pouvoir activer ou désactiver le blocage de l'accès public pour les AMI.

Table des matières

- [Paramètres par défaut](#)
- [Autorisations IAM requises](#)
- [Activer le blocage de l'accès public pour les AMI](#)
- [Désactiver le blocage de l'accès public pour les AMI](#)
- [Afficher l'état du blocage de l'accès public pour les AMI](#)

Paramètres par défaut

Le paramètre Bloquer l'accès public aux AMI est activé ou désactivé par défaut selon que votre compte est nouveau ou existant, et selon que vous possédez des AMI publiques. Le tableau suivant répertorie les paramètres par défaut :

AWS compte	Valeur par défaut du paramètre Bloquer l'accès public aux AMI
Nouveaux comptes	Activées
Comptes existants sans AMI publiques ¹	Activées
Comptes existants avec une ou plusieurs AMI publiques	Désactivées

¹ Si votre compte comportait une ou plusieurs AMI publiques le 15 juillet 2023 ou après cette date, le paramètre Bloquer l'accès public aux AMI est désactivé par défaut pour votre compte, même si vous avez ensuite rendu toutes les AMI privées.

Autorisations IAM requises

Pour utiliser le blocage de l'accès public pour les AMI, vous devez disposer des autorisations IAM suivantes :

- `EnableImageBlockPublicAccess`
- `DisableImageBlockPublicAccess`
- `GetImageBlockPublicAccessState`

Activer le blocage de l'accès public pour les AMI

Pour empêcher le partage public de vos AMI, vous pouvez activer le blocage de l'accès public pour les AMI au niveau du compte. Vous devez activer le blocage de l'accès public pour les AMI dans chaque Région AWS dans laquelle vous souhaitez empêcher le partage public de vos AMI. Si vous possédez déjà des AMI publiques, elles resteront accessibles au public.

Console

Pour activer le blocage de l'accès public pour les AMI dans la région spécifiée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez la région dans laquelle vous souhaitez activer le blocage de l'accès public pour les AMI.
3. Si le tableau de bord n'est pas affiché, dans le volet de navigation, choisissez Tableau de bord EC2.
4. Sous Attributs du compte, sélectionnez Protection et sécurité des données.
5. Sous Bloquer l'accès public pour les AMI, choisissez Gérer.
6. Cochez la case Bloquer le partage public, puis sélectionnez Mettre à jour.

Note

L'API peut prendre jusqu'à 10 minutes pour configurer ce paramètre. Pendant ce temps, la valeur est Nouveau partage public autorisé. Lorsque l'API a terminé la configuration, la valeur passe automatiquement à Nouveau partage public bloqué.

AWS CLI

Pour activer le blocage de l'accès public pour les AMI dans la région spécifiée

Utilisez la commande [enable-image-block-public-access](#) et spécifiez la région dans laquelle vous souhaitez activer le blocage de l'accès public pour les AMI. Pour le paramètre `--image-block-public-access-state`, spécifiez `block-new-sharing`.

```
aws ec2 enable-image-block-public-access \  
  --region us-east-1 \  
  --image-block-public-access-state block-new-sharing
```

Sortie attendue

```
{  
  "ImageBlockPublicAccessState": "block-new-sharing"  
}
```

Note

L'API peut prendre jusqu'à 10 minutes pour configurer ce paramètre. Pendant ce temps, si vous exécutez la commande [get-image-block-public-access-state](#), la réponse est `unblocked`. Lorsque l'API a terminé la configuration, la réponse est `block-new-sharing`.

Désactiver le blocage de l'accès public pour les AMI

Pour permettre aux utilisateurs de votre compte de partager publiquement vos AMI, désactivez le blocage de l'accès public au niveau du compte. Vous devez désactiver le blocage de l'accès public pour les AMI Région AWS dans chaque cas où vous souhaitez autoriser le partage public de vos AMI.

Console

Pour désactiver le blocage de l'accès public pour les AMI dans la région spécifiée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez la région dans laquelle vous souhaitez désactiver le blocage de l'accès public pour les AMI.

3. Si le tableau de bord n'est pas affiché, dans le volet de navigation, choisissez Tableau de bord EC2.
4. Sous Attributs du compte, sélectionnez Protection et sécurité des données.
5. Sous Bloquer l'accès public pour les AMI, choisissez Gérer.
6. Décochez la case Bloquer le partage public, puis sélectionnez Mettre à jour.
7. Saisissez **confirm** lorsque vous êtes invité à confirmer, puis choisissez Autoriser le partage public.

 Note

L'API peut prendre jusqu'à 10 minutes pour configurer ce paramètre. Pendant ce temps, la valeur est Nouveau partage public bloqué. Lorsque l'API a terminé la configuration, la valeur passe automatiquement à Nouveau partage public autorisé.

AWS CLI

Pour désactiver le blocage de l'accès public pour les AMI dans la région spécifiée

Utilisez la commande [disable-image-block-public-access](#) et spécifiez la région dans laquelle vous souhaitez désactiver le blocage de l'accès public pour les AMI.

```
aws ec2 disable-image-block-public-access --region us-east-1
```

Sortie attendue

```
{  
  "ImageBlockPublicAccessState": "unblocked"  
}
```

 Note

L'API peut prendre jusqu'à 10 minutes pour configurer ce paramètre. Pendant ce temps, si vous exécutez la commande [get-image-block-public-access-state](#), la réponse est `block-new-sharing`. Lorsque l'API a terminé la configuration, la réponse est `unblocked`.

Afficher l'état du blocage de l'accès public pour les AMI

Pour savoir si le partage public de vos AMI est bloqué dans votre compte, vous pouvez consulter l'état du blocage de l'accès public pour les AMI. Vous devez consulter l'état dans chaque Région AWS dans laquelle vous souhaitez voir si le partage public pour vos AMI est bloqué.

Console

Pour afficher l'état du blocage de l'accès public pour les AMI dans la région spécifiée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez la région dans laquelle vous souhaitez afficher l'état du blocage de l'accès public pour les AMI.
3. Si le tableau de bord n'est pas affiché, dans le volet de navigation, choisissez Tableau de bord EC2.
4. Sous Attributs du compte, sélectionnez Protection et sécurité des données.
5. Sous Bloquer l'accès public pour les AMI, vérifiez le champ Accès public. La valeur est Nouveau partage public bloqué ou Nouveau partage public autorisé.

AWS CLI

Pour obtenir l'état du blocage de l'accès public pour les AMI dans la région spécifiée

Utilisez la commande [get-image-block-public-access](#) et spécifiez la région dans laquelle vous souhaitez obtenir l'état du blocage de l'accès public pour les AMI.

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

Sortie attendue : la valeur est `block-new-sharing` ou `unblocked`.

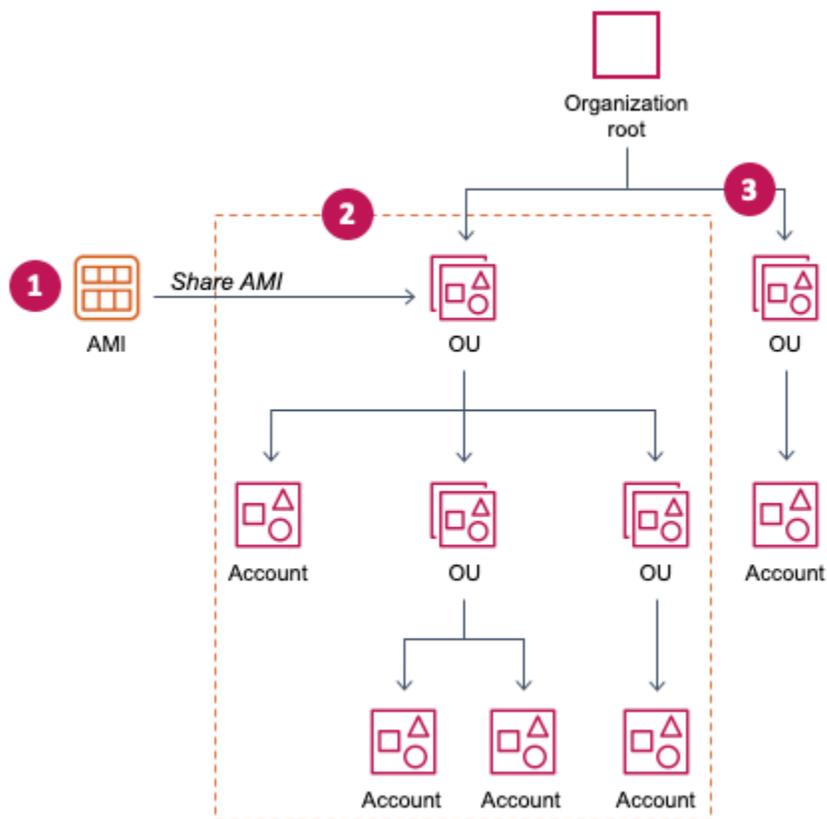
```
{  
  "ImageBlockPublicAccessState": "block-new-sharing"  
}
```

Partager une AMI avec des organisations ou des unités d'organisations spécifiques

[AWS Organizations](#) est un service de gestion de comptes qui vous permet de consolider plusieurs comptes au Comptes AWS sein d'une organisation que vous créez et gérez de manière centralisée. Vous pouvez partager une AMI avec une organisation ou une unité organisationnelle (UO) que vous avez créée, en plus de [la partager avec des comptes spécifiques](#).

L'organisation est une entité que vous créez pour consolider et gérer vos Comptes AWS de manière centralisée. Vous pouvez organiser les comptes dans une structure arborescente hiérarchique, avec une [racine](#) au sommet et des [unités organisationnelles](#) imbriquées sous la racine de l'organisation. Chaque compte peut directement être ajouté à la racine ou être placé dans l'une des UO de la hiérarchie. Pour en savoir plus, consultez la section [Terminologie et concepts relatifs àAWS Organizations](#) du Guide de l'utilisateur AWS Organizations .

Lorsque vous partagez une AMI avec une organisation ou une UO, tous les comptes enfants ont accès à l'AMI. Par exemple, dans le diagramme suivant, l'AMI est partagée avec une unité d'organisation de niveau supérieur (indiquée par la flèche au niveau du numéro 1). Toutes les UO et tous les comptes imbriqués sous cette UO de niveau supérieur (indiquée par la ligne pointillée au niveau du numéro 2) ont également accès à l'AMI. Les comptes de l'organisation et de l'UO en dehors de la ligne pointillée (indiqués par le numéro 3) n'ont pas accès à l'AMI car ils ne sont pas enfants de l'UO avec laquelle l'AMI est partagée.



Considérations

Tenez compte des éléments suivants lorsque vous partagez des AMI avec des organisations ou des unités organisationnelles spécifiques.

- **Propriété** : pour partager une AMI, votre Compte AWS doit être propriétaire de l'AMI.
- **Limites de partage** : le propriétaire de l'AMI peut partager une AMI avec n'importe quelle organisation ou unité d'organisation, y compris les organisations et les UO dont il n'est pas membre.

Pour connaître le nombre maximal d'entités avec lesquelles une AMI peut être partagée au sein d'une région, consultez les [quotas de service Amazon EC2](#).

- **Balises** : vous ne pouvez pas partager de balises définies par l'utilisateur (balises que vous associez à une AMI). Lorsque vous partagez une AMI, les balises définies par l'utilisateur ne sont accessibles au Compte AWS à aucun membre d'une organisation ou d'une unité d'organisation avec laquelle l'AMI est partagée.

- Format ARN : lorsque vous spécifiez une organisation ou une UO dans une commande, veillez à utiliser le format ARN approprié. Vous obtiendrez une erreur si vous spécifiez uniquement l'ID, par exemple si vous spécifiez uniquement `o-123example` ou `ou-1234-5example`.

Formats ARN corrects :

- ARN de l'organisation : `arn:aws:organizations::account-id:organization/organization-id`
- ARN de l'UO : `arn:aws:organizations::account-id:ou/organization-id/ou-id`

Où :

- *account-id* est le numéro de compte de gestion à 12 chiffres, par exemple, 123456789012. Si vous ne connaissez pas le numéro de compte de gestion, vous pouvez décrire l'organisation ou l'unité d'organisation pour obtenir l'ARN, qui inclut le numéro de compte de gestion. Pour plus d'informations, consultez [Obtenir l'ARN](#).
- *organization-id* est l'ID de l'organisation, par exemple, o-123example.
- *ou-id* est l'ID de l'unité d'organisation, par exemple, ou-1234-5example.

Pour plus d'informations sur le format des ARN, consultez [Amazon Resource Names \(ARN\)](#) dans le guide de l'utilisateur IAM.

- Chiffrement et clés : vous pouvez partager des AMI qui sont sauvegardées par des instantanés chiffrés et non chiffrés.
 - Les instantanés chiffrés doivent être chiffrés avec une clé gérée par le client. Vous ne pouvez pas partager d'AMI basées sur des instantanés chiffrés avec la clé AWS gérée par défaut.
 - Si vous partagez une AMI basée sur des instantanés chiffrés, vous devez autoriser les organisations ou les unités d'organisation à utiliser les clés gérées par le client qui ont été utilisées pour chiffrer les instantanés. Pour plus d'informations, consultez [Autoriser les organisations et les unités d'organisation à utiliser une clé KMS](#).
- Région : les AMI constituent une ressource régionale. Lorsque vous partagez une AMI, elle est uniquement disponible dans la région à partir de laquelle vous l'avez partagée. Pour rendre une AMI disponible dans une autre région, copiez-la dans la région souhaitée puis partagez-la. Pour plus d'informations, consultez [Copier une AMI](#).
- Utilisation : lorsque vous partagez une AMI, les utilisateurs peuvent uniquement lancer des instances à partir de l'AMI. Ils ne peuvent pas la supprimer, la partager ou la modifier. Toutefois, après avoir lancé une instance à l'aide de votre AMI, ils peuvent créer une AMI à partir de l'instance lancée.

- Facturation : vous n'êtes pas facturé lorsque votre AMI est utilisée par d'autres personnes Comptes AWS pour lancer des instances. Les comptes qui lancent des instances à l'aide de l'AMI sont facturés pour les instances qu'ils lancent.

Autoriser les organisations et les unités d'organisation à utiliser une clé KMS

Si vous partagez une AMI basée sur des instantanés chiffrés, vous devez également autoriser les organisations ou les unités d'organisation à utiliser celles AWS KMS keys qui ont été utilisées pour chiffrer les instantanés.

Utilisez les `aws:PrincipalOrgPaths` touches `aws:PrincipalOrgID` et pour comparer le AWS Organizations chemin du principal qui fait la demande avec le chemin indiqué dans la politique. Ce principal peut être un utilisateur, un rôle IAM, un utilisateur fédéré ou un utilisateur Compte AWS root. Dans une politique, cette clé de condition vérifie que le demandeur est un membre du compte au sein de l'organisation racine ou des unités d'organisation spécifiées dans AWS Organizations. Pour plus d'exemples de déclarations de condition, consultez [aws:PrincipalOrgID](#) et [aws:PrincipalOrgPaths](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur la modification d'une politique clé, voir [Autoriser les utilisateurs d'autres comptes à utiliser une clé KMS](#) dans le Guide du AWS Key Management Service développeur.

Pour accorder à une organisation ou à une unité d'organisation l'autorisation d'utiliser une clé KMS, ajoutez l'instruction suivante à la politique de clé.

```
{
  "Sid": "Allow access for organization root",
  "Effect": "Allow",
  "Principal": "*",
  "Action": [
    "kms:Describe*",
    "kms:List*",
    "kms:Get*",
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
```

```
        "aws:PrincipalOrgID": "o-123example"  
    }  
  }  
}
```

Pour partager une clé KMS avec plusieurs unités d'organisation, vous pouvez utiliser une politique similaire à l'exemple suivant.

```
{  
  "Sid": "Allow access for specific OUs and their descendants",  
  "Effect": "Allow",  
  "Principal": "*",  
  "Action": [  
    "kms:Describe*",  
    "kms:List*",  
    "kms:Get*",  
    "kms:Encrypt",  
    "kms:Decrypt",  
    "kms:ReEncrypt*",  
    "kms:GenerateDataKey*"  
  ],  
  "Resource": "*",  
  "Condition": {  
    "StringEquals": {  
      "aws:PrincipalOrgID": "o-123example"  
    },  
    "ForAnyValue:StringLike": {  
      "aws:PrincipalOrgPaths": [  
        "o-123example/r-ab12/ou-ab12-33333333/*",  
        "o-123example/r-ab12/ou-ab12-22222222/*"  
      ]  
    }  
  }  
}
```

Partager une AMI

Vous pouvez utiliser la console Amazon EC2 ou AWS CLI pour partager une AMI avec une organisation ou une unité d'organisation.

Partager une AMI (console)

Pour partager une AMI avec une organisation ou une unité d'organisation à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Sélectionnez votre AMI dans la liste, puis choisissez Actions (Actions), Edit AMI permissions (Modifier des autorisations d'AMI).
4. Sous AMI availability (Disponibilité de l'AMI), choisissez Private (Privée).
5. En regard de Shared organizations/OUs (Organisations/UO partagées), choisissez Add organization/OU ARN (Ajouter un ARN d'organisation/d'UO).
6. Pour Organization/OU ARN (ARN d'organisation/d'UO), saisissez l'ARN de l'organisation ou de l'UO avec laquelle vous souhaitez partager l'AMI, puis choisissez Share AMI (Partager l'AMI). Notez que vous devez spécifier l'ARN complet, pas seulement l'ID.

Pour partager cette AMI avec plusieurs organisations ou UO, répétez cette étape jusqu'à avoir ajouté toutes les organisations ou UO requises.

Note

Vous n'avez pas besoin de partager les instantanés (snapshots) Amazon EBS qu'une AMI référence afin de partager l'AMI. Seule l'AMI elle-même doit être partagée, et le système fournit automatiquement à l'instance l'accès aux instantanés Amazon EBS référencés pour le lancement. Toutefois, vous devez partager les clés KMS utilisées pour chiffrer les instantanés auxquels l'AMI fait référence. Pour plus d'informations, consultez [Autoriser les organisations et les unités d'organisation à utiliser une clé KMS](#).

7. Lorsque vous avez terminé, sélectionnez Save Changes (Enregistrer les modifications).
8. (Facultatif) Pour afficher les organisations ou les UO avec lesquelles vous avez partagé l'AMI, sélectionnez l'AMI dans la liste, choisissez l'onglet Permissions (Autorisations) et faites défiler l'écran jusqu'à Shared organizations/OUs (Organisations/UO partagées). Pour trouver les AMI partagées avec vous, consultez [Rechercher des AMI partagées](#).

Partager une AMI (Outils pour Windows PowerShell)

Utilisez la [Edit-EC2ImageAttribute](#) commande (Outils pour Windows PowerShell) pour partager une AMI, comme indiqué dans les exemples suivants.

Pour partager une AMI avec une organisation ou une unité d'organisation

La commande suivante accorde des autorisations de lancement pour l'AMI spécifiée à l'organisation spécifiée.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -  
Attribute launchPermission -OperationType add -OrganizationArn  
"arn:aws:organizations::123456789012:organization/o-123example"
```

Note

Vous n'avez pas besoin de partager les instantanés (snapshots) Amazon EBS qu'une AMI référence afin de partager l'AMI. Seule l'AMI elle-même doit être partagée, et le système fournit automatiquement à l'instance l'accès aux instantanés Amazon EBS référencés pour le lancement. Toutefois, vous n'avez pas besoin de partager les clés KMS utilisées pour chiffrer les instantanés référencés par l'AMI. Pour plus d'informations, consultez [Autoriser les organisations et les unités d'organisation à utiliser une clé KMS](#).

Pour arrêter le partage d'une AMI avec une organisation ou une unité d'organisation

La commande suivante supprime les autorisations de lancement pour l'AMI spécifiée dans l'organisation spécifiée :

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -  
Attribute launchPermission -OperationType remove -OrganizationArn  
"arn:aws:organizations::123456789012:organization/o-123example"
```

Pour arrêter de partager une AMI avec toutes les organisations, unités d'organisation et Comptes AWS

La commande suivante retire toutes les autorisations de lancement publiques et explicites pour l'AMI spécifiée. Veuillez noter que le propriétaire de l'AMI dispose toujours d'autorisations de lancement et n'est, par conséquent, pas affecté par cette commande.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute  
launchPermission
```

Partager une AMI (AWS CLI)

Utilisez la commande [modify-image-attribute](#) (AWS CLI) pour partager une AMI.

Pour partager une AMI avec une organisation à l'aide du AWS CLI

La commande [modify-image-attribute](#) accorde des autorisations de lancement pour l'AMI spécifiée à l'organisation spécifiée. Notez que vous devez spécifier l'ARN complet, pas seulement l'ID.

```
aws ec2 modify-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --launch-permission  
  "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/  
o-123example}]"
```

Pour partager une AMI avec une unité d'organisation à l'aide du AWS CLI

La commande [modify-image-attribute](#) accorde des autorisations de lancement pour l'AMI spécifiée à l'unité d'organisation spécifiée. Notez que vous devez spécifier l'ARN complet, pas seulement l'ID.

```
aws ec2 modify-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --launch-permission  
  "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/  
ou-1234-5example}]"
```

Note

Vous n'avez pas besoin de partager les instantanés (snapshots) Amazon EBS qu'une AMI référence afin de partager l'AMI. Seule l'AMI elle-même doit être partagée, et le système fournit automatiquement à l'instance l'accès aux instantanés Amazon EBS référencés pour le lancement. Toutefois, vous n'avez pas besoin de partager les clés KMS utilisées pour chiffrer les instantanés référencés par l'AMI. Pour plus d'informations, consultez [Autoriser les organisations et les unités d'organisation à utiliser une clé KMS](#).

Arrêter le partage d'une AMI

Vous pouvez utiliser la console Amazon EC2 ou le AWS CLI pour arrêter de partager une AMI avec une organisation ou une unité d'organisation.

Arrêter le partage d'une AMI (console)

Pour arrêter le partage d'une AMI avec une organisation ou une unité d'organisation à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Sélectionnez votre AMI dans la liste, puis choisissez Actions (Actions), Edit AMI permissions (Modifier des autorisations d'AMI).
4. Sous Shared organizations/OUs (Organisations/UO partagées), sélectionnez les organisations ou les unités d'organisation avec lesquelles vous souhaitez arrêter de partager l'AMI, puis choisissez Remove Selected (Retirer l'élément sélectionné).
5. Lorsque vous avez terminé, sélectionnez Save Changes (Enregistrer les modifications).
6. (Facultatif) Pour vérifier que vous avez arrêté de partager l'AMI avec les organisations ou les UO souhaitées, sélectionnez l'AMI dans la liste, choisissez l'onglet Permissions (Autorisations) et faites défiler l'écran jusqu'à Shared organizations/OUs (Organisations/UO partagées).

Arrêter le partage d'une AMI (AWS CLI)

Utilisez les commandes [modify-image-attribute](#) ou [reset-image-attribute](#) (AWS CLI) pour arrêter le partage d'une AMI.

Pour arrêter de partager une AMI avec une organisation ou une unité d'organisation à l'aide du AWS CLI

La commande [modify-image-attribute](#) supprime les autorisations de lancement pour l'AMI spécifiée de l'organisation spécifiée. Notez que vous devez spécifier l'ARN.

```
aws ec2 modify-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --launch-permission  
  "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/  
o-123example}]"
```

Pour arrêter de partager une AMI avec toutes les organisations et unités d'organisation et Comptes AWS d'utiliser le AWS CLI

La commande [reset-image-attribute](#) supprime toutes les autorisations de lancement publiques et explicites pour l'AMI spécifiée. Veuillez noter que le propriétaire de l'AMI dispose toujours d'autorisations de lancement et n'est, par conséquent, pas affecté par cette commande.

```
aws ec2 reset-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --attribute launchPermission
```

Note

Vous ne pouvez pas arrêter le partage d'une AMI avec un compte spécifique si elle se trouve dans une organisation ou une unité d'organisation avec laquelle une AMI est partagée. Si vous essayez d'arrêter le partage de l'AMI en supprimant les autorisations de lancement du compte, Amazon EC2 renvoie un message de succès. Toutefois, l'AMI continue d'être partagée avec le compte.

Afficher les organisations et les UO avec lesquelles une AMI est partagée

Vous pouvez utiliser la console Amazon EC2 ou le AWS CLI pour vérifier avec quelles organisations et unités d'organisation vous avez partagé votre AMI.

Afficher les organisations et les UO avec lesquelles une AMI est partagée (console)

Pour vérifier avec quelles organisations et quelles UO vous avez partagé votre AMI à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Sélectionnez votre AMI dans la liste, choisissez l'onglet Permissions (Autorisations) et faites défiler l'écran jusqu'à Shared organizations/OUs (Organisations/UO partagées).

Pour trouver les AMI partagées avec vous, consultez [Rechercher des AMI partagées](#).

Afficher les organisations et les UO avec lesquelles une AMI est partagée (AWS CLI)

Vous pouvez vérifier avec quelles organisations et unités d'organisation vous avez partagé votre AMI à l'aide de la commande [describe-image-attribute](#) (AWS CLI) et de l'attribut `launchPermission`.

Pour vérifier avec quelles organisations et unités d'organisation vous avez partagé votre AMI à l'aide du AWS CLI

La commande [describe-image-attribute](#) décrit l'attribut `launchPermission` pour l'AMI spécifiée et renvoie les organisations et les unités d'organisation avec lesquelles vous avez partagé l'AMI.

```
aws ec2 describe-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --attribute launchPermission
```

Exemple de réponse

```
{  
  "ImageId": "ami-0abcdef1234567890",  
  "LaunchPermissions": [  
    {  
      "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/  
o-123example/ou-1234-5example"  
    }  
  ]  
}
```

Obtenir l'ARN

Les ARN de l'organisation et de l'unité d'organisation contiennent le numéro de compte de gestion à 12 chiffres. Si vous ne connaissez pas le numéro de compte de gestion, vous pouvez décrire l'organisation ou l'unité d'organisation pour obtenir l'ARN de chacune. Dans les exemples suivants, 123456789012 est le numéro du compte de gestion.

Avant de pouvoir obtenir les ARN, vous devez être autorisé à décrire les organisations et les unités d'organisations. La politique suivante fournit l'autorisation nécessaire.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "organizations:Describe*"  
      ],  
    }  
  ],  
}
```

```
        "Resource": "*"
    }
  ]
}
```

Pour obtenir l'ARN d'une organisation

Utilisez la commande [describe-organization](#) et le paramètre `--query` défini sur `'Organization.Arn'` pour renvoyer uniquement l'ARN de l'organisation.

```
aws organizations describe-organization --query 'Organization.Arn'
```

Exemple de réponse

```
"arn:aws:organizations::123456789012:organization/o-123example"
```

Pour obtenir l'ARN d'une unité d'organisation

Utilisez la commande [describe-organizational-unit](#), spécifiez l'ID de l'unité d'organisation et définissez le paramètre `--query` sur `'OrganizationalUnit.Arn'` pour renvoyer uniquement l'ARN de l'unité d'organisation.

```
aws organizations describe-organizational-unit --organizational-unit-id ou-1234-5example --query 'OrganizationalUnit.Arn'
```

Exemple de réponse

```
"arn:aws:organizations::123456789012:ou/o-123example/ou-1234-5example"
```

Partager une AMI avec des comptes AWS spécifiques

Vous pouvez partager une AMI avec un utilisateur spécifique Comptes AWS sans la rendre publique. Tout ce dont vous avez besoin, ce sont les Compte AWS pièces d'identité.

Un Compte AWS identifiant est un numéro à 12 chiffres, par exemple 012345678901, qui identifie de manière unique un Compte AWS. Pour plus d'informations, veuillez consulter la section [Afficher les identifiants Compte AWS](#) dans le Guide de référence AWS Account Management .

Considérations

Tenez compte des points suivants lorsque vous partagez des AMI avec des personnes spécifiques Comptes AWS.

- **Propriété** : pour partager une AMI, votre Compte AWS doit être propriétaire de l'AMI.
- **Sharing limits (Limites de partage)** : pour connaître le nombre maximal d'entités avec lesquelles une AMI peut être partagée au sein d'une région, consultez les [quotas de service Amazon EC2](#).
- **Balises** : vous ne pouvez pas partager de balises définies par l'utilisateur (balises que vous associez à une AMI). Lorsque vous partagez une AMI, les balises définies par l'utilisateur ne sont pas accessibles aux personnes avec Compte AWS auxquelles l'AMI est partagée.
- **Chiffrement et clés** : vous pouvez partager des AMI qui sont sauvegardées par des instantanés chiffrés et non chiffrés.
 - Les instantanés chiffrés doivent être chiffrés avec une clé KMS. Vous ne pouvez pas partager d'AMI sauvegardées par des instantanés qui sont chiffrés avec la clé gérée par AWS par défaut.
 - Si vous partagez une AMI basée sur des instantanés chiffrés, vous devez Comptes AWS autoriser l'utilisation des clés KMS utilisées pour chiffrer les instantanés. Pour plus d'informations, consultez [Autoriser les organisations et les unités d'organisation à utiliser une clé KMS](#). Pour configurer la politique de clé dont vous avez besoin pour lancer des instances Auto Scaling lorsque vous utilisez une clé gérée par le client pour le chiffrement, consultez la section [AWS KMS key Politique requise pour une utilisation avec des volumes chiffrés](#) dans le guide de l'utilisateur Amazon EC2 Auto Scaling.
- **Région** : les AMI constituent une ressource régionale. Lorsque vous partagez une AMI, elle n'est disponible que dans la région concernée. Pour rendre une AMI disponible dans une autre région, copiez-la dans la région souhaitée puis partagez-la. Pour plus d'informations, consultez [Copier une AMI](#).
- **Utilisation** : lorsque vous partagez une AMI, les utilisateurs peuvent uniquement lancer des instances à partir de l'AMI. Ils ne peuvent pas la supprimer, la partager ou la modifier. Toutefois, une fois qu'ils ont lancé une instance à l'aide de votre AMI, ils peuvent alors créer une AMI à partir de leur instance.
- **Copie d'AMI partagées** : si les utilisateurs d'un autre compte souhaitent copier une AMI partagée, vous devez leur accorder des autorisations de lecture pour le stockage qui sauvegarde l'AMI. Pour plus d'informations, consultez [Copie entre comptes](#).

- Facturation : vous n'êtes pas facturé lorsque votre AMI est utilisée par d'autres personnes Comptes AWS pour lancer des instances. Les comptes qui lancent des instances à l'aide de l'AMI sont facturés pour les instances qu'ils lancent.

Partager une AMI (console)

Pour donner des autorisations de lancement explicites à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Sélectionnez votre AMI dans la liste, puis choisissez Actions (Actions), Edit AMI permissions (Modifier des autorisations d'AMI).
4. Choisissez Private (Privé).
5. Sous Shared accounts (Comptes partagés), choisissez Add account ID (Ajouter un ID de compte).
6. Dans Compte AWS ID, entrez l' Compte AWS ID avec lequel vous souhaitez partager l'AMI, puis choisissez Partager l'AMI.

Pour partager cette AMI avec plusieurs comptes, répétez les étapes 5 et 6 jusqu'à ce que vous ayez ajouté tous les identifiants de compte requis.

Note

Vous n'avez pas besoin de partager les instantanés (snapshots) Amazon EBS qu'une AMI référence afin de partager l'AMI. Seule l'AMI elle-même doit être partagée. Le système permet automatiquement à l'instance d'accéder aux instantanés (snapshots) Amazon EBS référencés pour le lancement. Toutefois, vous n'avez pas besoin de partager les clés Clés KMS utilisées pour chiffrer les instantanés référencés par l'AMI. Pour plus d'informations, consultez [Partager un instantané Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

7. Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).
8. (Facultatif) Pour afficher les Compte AWS identifiants avec lesquels vous avez partagé l'AMI, sélectionnez l'AMI dans la liste, puis cliquez sur l'onglet Autorisations. Pour trouver les AMI partagées avec vous, consultez [Rechercher des AMI partagées](#).

Partager une AMI (Outils pour Windows PowerShell)

Utilisez la [Edit-EC2ImageAttribute](#) commande (Outils pour Windows PowerShell) pour partager une AMI, comme indiqué dans les exemples suivants.

Pour donner des autorisations de lancement explicites

La commande suivante donne au Compte AWS spécifié des autorisations de lancement pour l'AMI spécifiée. Dans l'exemple suivant, remplacez l'exemple d'ID d'AMI par un ID d'AMI valide et remplacez-le *account-id* par l' Compte AWS ID à 12 chiffres.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute  
launchPermission -OperationType add -UserId "account-id"
```

Note

Vous n'avez pas besoin de partager les instantanés (snapshots) Amazon EBS qu'une AMI référence afin de partager l'AMI. Seule l'AMI elle-même doit être partagée. Le système permet automatiquement à l'instance d'accéder aux instantanés (snapshots) Amazon EBS référencés pour le lancement. Toutefois, vous n'avez pas besoin de partager les clés Clés KMS utilisées pour chiffrer les instantanés référencés par l'AMI. Pour plus d'informations, consultez [Partager un instantané Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Pour supprimer des autorisations de lancement données à un compte

La commande suivante supprime les autorisations de lancement de l'AMI spécifié pour le Compte AWS spécifié. Dans l'exemple suivant, remplacez l'exemple d'ID d'AMI par un ID d'AMI valide et remplacez-le *account-id* par l' Compte AWS ID à 12 chiffres.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute  
launchPermission -OperationType remove -UserId "account-id"
```

Pour supprimer toutes les autorisations de lancement

La commande suivante retire toutes les autorisations de lancement publiques et explicites pour l'AMI spécifiée. Veuillez noter que le propriétaire de l'AMI dispose toujours d'autorisations de lancement et n'est, par conséquent, pas affecté par cette commande. Dans l'exemple suivant, remplacez l'exemple d'identifiant d'AMI par un ID d'AMI valide.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute  
LaunchPermission
```

Partager une AMI (AWS CLI)

Utilisez la commande [modify-image-attribute](#) (AWS CLI) pour partager une AMI comme illustré dans les exemples suivants.

Pour donner des autorisations de lancement explicites

La commande suivante donne au Compte AWS spécifié des autorisations de lancement pour l'AMI spécifiée. Dans l'exemple suivant, remplacez l'exemple d'ID d'AMI par un ID d'AMI valide et remplacez-le *account-id* par l' Compte AWS ID à 12 chiffres.

```
aws ec2 modify-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --launch-permission "Add=[{UserId=account-id}]"
```

Note

Vous n'avez pas besoin de partager les instantanés (snapshots) Amazon EBS qu'une AMI référence afin de partager l'AMI. Seule l'AMI elle-même doit être partagée. Le système permet automatiquement à l'instance d'accéder aux instantanés (snapshots) Amazon EBS référencés pour le lancement. Toutefois, vous n'avez pas besoin de partager les clés Clés KMS utilisées pour chiffrer les instantanés référencés par l'AMI. Pour plus d'informations, consultez [Partager un instantané Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Pour supprimer des autorisations de lancement données à un compte

La commande suivante supprime les autorisations de lancement de l'AMI spécifié pour le Compte AWS spécifié. Dans l'exemple suivant, remplacez l'exemple d'ID d'AMI par un ID d'AMI valide et remplacez-le *account-id* par l' Compte AWS ID à 12 chiffres.

```
aws ec2 modify-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --launch-permission "Remove=[{UserId=account-id}]"
```

Pour supprimer toutes les autorisations de lancement

La commande suivante retire toutes les autorisations de lancement publiques et explicites pour l'AMI spécifiée. Veuillez noter que le propriétaire de l'AMI dispose toujours d'autorisations de lancement et n'est, par conséquent, pas affecté par cette commande. Dans l'exemple suivant, remplacez l'exemple d'identifiant d'AMI par un ID d'AMI valide.

```
aws ec2 reset-image-attribute \  
  --image-id ami-0abcdef1234567890 \  
  --attribute launchPermission
```

Annuler le partage d'une AMI avec votre Compte AWS

Une Amazon Machine Image (AMI) peut être [partagée avec des Comptes AWS spécifiques](#) en ajoutant les comptes aux autorisations de lancement de l'AMI. Si une AMI a été partagée avec votre Compte AWS et que vous ne souhaitez plus qu'elle soit partagée avec votre compte, vous pouvez supprimer votre compte des autorisations de lancement de l'AMI. Pour ce faire, exécutez la `cancel-image-launch-permission` AWS CLI commande. Lorsque vous exécutez cette commande, votre Compte AWS est privé des autorisations de lancement pour l'AMI spécifiée.

Vous pouvez annuler le partage d'une AMI avec votre compte, par exemple pour réduire la probabilité de lancer une instance avec une AMI inutilisée ou obsolète qui a été partagée avec vous. Lorsque vous annulez le partage d'une AMI avec votre compte, celle-ci n'apparaît plus dans les listes d'AMI de la console EC2 ni dans la sortie de [describe-images](#) (langue française non garantie).

Rubriques

- [Limites](#)
- [Annulation du partage d'une AMI avec votre compte](#)
- [Trouver les AMI partagées avec votre compte](#)

Limites

- Vous pouvez supprimer votre compte des autorisations de lancement d'une AMI partagée Compte AWS uniquement avec vous. Vous ne pouvez pas utiliser `cancel-image-launch-permission` pour supprimer votre compte des autorisations de lancement d'une [AMI partagée avec une organisation ou une unité d'organisation \(OU\)](#) ou pour supprimer l'accès aux AMI publiques.
- Vous ne pouvez pas supprimer définitivement votre compte des autorisations de lancement d'une AMI. Un propriétaire d'AMI peut à nouveau partager une AMI avec votre compte.

- Les AMI constituent une ressource régionale. Lors de l'exécution de `cancel-image-launch-permission`, vous devez spécifier la région dans laquelle se trouve l'AMI. Vous pouvez soit spécifier la région dans la commande, soit utiliser la [variable d'environnement](#) `AWS_DEFAULT_REGION`.
- Seuls les SDK AWS CLI et permettent de supprimer votre compte des autorisations de lancement d'une AMI. La console EC2 ne prend pas actuellement en charge cette fonction.

Annulation du partage d'une AMI avec votre compte

Note

Une fois que vous avez annulé le partage d'une AMI avec votre compte, vous ne pouvez pas le rétablir. Pour rétablir l'accès à l'AMI, le propriétaire de l'AMI doit la partager avec votre compte.

AWS CLI

Pour annuler le partage d'une AMI avec votre Compte AWS

Utilisez la commande [cancel-image-launch-permission](#) et spécifiez l'ID d'AMI.

```
aws ec2 cancel-image-launch-permission \  
  --image-id ami-0123456789example \  
  --region us-east-1
```

Sortie attendue

```
{  
  "Return": true  
}
```

PowerShell

Pour annuler le partage d'une AMI avec vous à Compte AWS l'aide du AWS Tools for PowerShell

Utilisez la commande [Stop-EC2ImageLaunchPermission](#) et spécifiez l'ID d'AMI.

```
Stop-EC2ImageLaunchPermission `
```

```
-ImageId ami-0123456789example `
-Region us-east-1
```

Sortie attendue

```
True
```

Trouver les AMI partagées qavec votre compte

Pour trouver les AMI partagées avec vous Compte AWS, consultez [Rechercher des AMI partagées](#).

Utiliser des signets

Si vous avez créé une AMI publique ou partagé une AMI avec une autre Compte AWS, vous pouvez créer un signet qui permet à un utilisateur d'accéder à votre AMI et de lancer immédiatement une instance dans son propre compte. C'est une façon simple de partager des références d'AMI afin que les utilisateurs n'aient pas à passer du temps à trouver votre AMI en vue de l'utiliser.

Veillez noter que votre AMI doit être publique, ou que vous devez l'avoir partagée avec l'utilisateur à qui vous souhaitez envoyer le marque-page.

Pour créer un marque-page pour votre AMI

1. Saisissez une URL avec les informations suivantes dans lesquelles Région correspond à la région dans laquelle votre AMI réside :

```
https://console.aws.amazon.com/ec2/v2/home?
region=region#LaunchInstanceWizard:ami=ami_id
```

Par exemple, cette URL lance une instance de l'AMI `ami-0abcdef1234567890` dans la région `us-east-1` USA Est (Virginie du Nord) :

```
https://console.aws.amazon.com/ec2/v2/home?region=us-
east-1#LaunchInstanceWizard:ami=ami-0abcdef1234567890
```

2. Communiquez le lien aux utilisateurs qui souhaitent utiliser votre AMI.
3. Pour utiliser un marque-page, choisissez le lien ou effectuez un copier-coller dans votre navigateur. L'assistant de lancement s'ouvre avec l'AMI déjà sélectionnée.

Consignes pour les AMI Linux partagées

Utilisez les consignes suivantes pour réduire la surface d'attaque et améliorer la fiabilité des AMI que vous créez.

Important

Aucune liste de consignes de sécurité ne peut être exhaustive. Créez vos AMI partagées avec soin et prenez le temps d'étudier où vous exposez peut-être des données sensibles.

Table des matières

- [Mise à jour des outils AMI avant leur utilisation](#)
- [Désactivation des connexions distantes basées sur un mot de passe pour l'utilisateur root](#)
- [Désactivation de l'accès local à la racine](#)
- [Suppression des paires de clés de l'hôte SSH](#)
- [Installation d'informations d'identification publiques](#)
- [Désactiver les vérifications DNS sshd \(facultatif\)](#)
- [Vous protéger](#)

Si vous créez des AMI pour AWS Marketplace, consultez la section [Bonnes pratiques en matière de création d'AMI](#) dans le Guide du AWS Marketplace vendeur pour connaître les directives, les politiques et les meilleures pratiques.

Pour plus d'informations sur la façon de partager des AMI en toute sécurité, consultez les articles suivants :

- [How To Share and Use Public AMIs in A Secure Manner](#)
- [Public AMI Publishing: Hardening and Clean-up Requirements](#)

Mise à jour des outils AMI avant leur utilisation

Pour les AMI basées sur un stockage d'instances, nous recommandons que vos AMI téléchargent et mettent à jour les outils de création AMI Amazon EC2 avant de les utiliser. Cela garantit que les nouvelles AMI basées sur vos AMI partagées disposent des derniers outils AMI.

Pour [Amazon Linux 2](#), installez le package `aws-amitools-ec2` et ajoutez les outils AMI à votre variable `PATH` avec la commande suivante. Pour [Amazon Linux AMI](#), le package `aws-amitools-ec2` est déjà installé par défaut.

```
[ec2-user ~]$ sudo yum install -y aws-amitools-ec2 && export PATH=$PATH:/opt/aws/bin
> /etc/profile.d/aws-amitools-ec2.sh && . /etc/profile.d/aws-amitools-ec2.sh
```

Mettez à niveau les outils AMI avec la commande suivante :

```
[ec2-user ~]$ sudo yum upgrade -y aws-amitools-ec2
```

Pour les autres distributions, assurez-vous que vous disposez des derniers outils AMI.

Désactivation des connexions distantes basées sur un mot de passe pour l'utilisateur root

En utilisant un mot de passe racine fixe pour une AMI publique, un risque de sécurité peut rapidement apparaître. Même le fait de compter sur les utilisateurs pour changer le mot de passe après leur première connexion laisse une petite place à une opportunité d'abus potentiel.

Pour résoudre ce problème, désactivez les connexions à distance basées sur mot de passe pour l'utilisateur racine.

Pour désactiver les connexions à distance basées sur un mot de passe pour l'utilisateur root

1. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte et localisez la ligne suivante :

```
#PermitRootLogin yes
```

2. Changez la ligne en :

```
PermitRootLogin without-password
```

L'emplacement de ce fichier de configuration peut varier pour votre distribution, ou si vous n'exécutez pas OpenSSH. Si tel est le cas, consultez la documentation appropriée.

Désactivation de l'accès local à la racine

Lorsque vous travaillez avec des AMI partagées, une bonne pratique consiste à désactiver les connexions directes à la racine. Pour ce faire, connectez-vous à votre instance en cours d'exécution et entrez la commande suivante :

```
[ec2-user ~]$ sudo passwd -l root
```

Note

Cette commande n'a pas d'impact sur l'utilisation de sudo.

Suppression des paires de clés de l'hôte SSH

Si vous prévoyez de partager une AMI issue d'une AMI publique, supprimez les paires de clés de l'hôte SSH existantes situées dans `/etc/ssh`. Cela force SSH à générer de nouvelles paires de clés SSH uniques lorsque quelqu'un lance une instance utilisant votre AMI, ce qui améliore la sécurité et réduit la probabilité d'attaques MITM.

Supprimez tous les fichiers clés suivants présents dans votre système.

- `ssh_host_dsa_key`
- `ssh_host_dsa_key.pub`
- `ssh_host_key`
- `ssh_host_key.pub`
- `ssh_host_rsa_key`
- `ssh_host_rsa_key.pub`
- `ssh_host_ecdsa_key`
- `ssh_host_ecdsa_key.pub`
- `ssh_host_ed25519_key`
- `ssh_host_ed25519_key.pub`

Vous pouvez supprimer tous ces fichiers en toute sécurité avec la commande suivante.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

⚠ Warning

Les utilitaires de suppression sécurisée tels que **shred** peuvent ne pas supprimer toutes les copies d'un fichier de vos supports de stockage. Des copies cachées de fichiers peuvent être créées par les systèmes de fichiers de journalisation (dont Amazon Linux default ext4), les instantanés (snapshots), les sauvegardes, RAID et la mise en cache temporaire. Pour plus d'informations, consultez la [documentation shred](#).

⚠ Important

Si vous oubliez de supprimer les paires de clés de l'hôte SSH existantes de votre AMI publique, notre processus routinier d'audit vous informe ainsi que tous les clients exécutant des instances de votre AMI du risque de sécurité potentiel. Au terme d'une courte période de grâce, nous marquons l'AMI comme privée.

Installation d'informations d'identification publiques

Après avoir configuré l'AMI pour empêcher la connexion à l'aide d'un mot de passe, vous devez vous assurer que les utilisateurs peuvent se connecter à l'aide d'un autre mécanisme.

Amazon EC2 permet aux utilisateurs de spécifier un nom de paire de clés publique-privée au moment de lancer une instance. Lorsqu'un nom de paire de clés valide est fourni à l'appel de l'API `RunInstances` (ou par les outils API de ligne de commande), la clé publique (la portion de la paire de clés qu'Amazon EC2 conserve sur le serveur après un appel à `CreateKeyPair` ou `ImportKeyPair`) est rendue disponible pour l'instance via une requête HTTP sur les métadonnées d'instance.

Pour se connecter via SSH, votre AMI doit récupérer la valeur clé au moment du démarrage et la joindre à `/root/.ssh/authorized_keys` (ou l'équivalent pour tout autre compte utilisateur sur l'AMI). Les utilisateurs peuvent lancer des instances de votre AMI avec votre paire de clés et se connecter sans avoir besoin de mot de passe racine.

De nombreuses distributions, dont Amazon Linux et Ubuntu, utilisent le package `cloud-init` pour injecter des informations d'identification de clé publiques pour un utilisateur configuré. Si votre distribution ne prend pas en charge `cloud-init`, vous pouvez ajouter le code suivant à un script de

démarrage système (tel que `/etc/rc.local`) pour extraire la clé publique que vous avez spécifiée au lancement pour l'utilisateur racine.

Note

Dans l'exemple suivant, l'adresse IP `http://169.254.169.254/` est une adresse lien-local et elle n'est valide que depuis l'instance.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
    mkdir -p /root/.ssh
    chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
    cat /tmp/my-key >> /root/.ssh/authorized_keys
    chmod 700 /root/.ssh/authorized_keys
    rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
    mkdir -p /root/.ssh
    chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
    cat /tmp/my-key >> /root/.ssh/authorized_keys
    chmod 700 /root/.ssh/authorized_keys
    rm /tmp/my-key
fi
```

Cela peut être appliqué à n'importe quel utilisateur. Il n'est pas nécessaire de la limiter à l'utilisateur `root`.

Note

La création d'un nouveau bundle d'une instance basée sur cette AMI inclut la clé avec laquelle elle a été lancée. Pour éviter l'inclusion de la clé, vous devez vider (ou supprimer) le fichier `authorized_keys` ou exclure ce fichier du nouveau bundle.

Désactiver les vérifications DNS sshd (facultatif)

Désactiver les vérifications DNS sshd affaiblit quelque peu votre sécurité sshd. Toutefois, si la résolution DNS échoue, les connexions SSH continuent de fonctionner. Si vous ne désactivez pas les vérifications sshd, les échecs de résolution DNS empêchent toutes les connexions.

Pour désactiver les vérifications DNS sshd

1. Ouvrez le fichier `/etc/ssh/sshd_config` dans un éditeur de texte et localisez la ligne suivante :

```
#UseDNS yes
```

2. Changez la ligne en :

```
UseDNS no
```

Note

L'emplacement de ce fichier de configuration peut varier pour votre distribution, ou si vous n'exécutez pas OpenSSH. Si tel est le cas, consultez la documentation appropriée.

Vous protéger

Nous déconseillons de stocker des données ou logiciels sensibles sur toute AMI que vous partagez. Les utilisateurs qui lancent une AMI partagée peuvent être en mesure de la regrouper et de l'enregistrer comme étant la leur. Suivez ces consignes pour vous permettre d'éviter de vous exposer à des risques de sécurité facilement négligés :

- Nous recommandons d'utiliser l'option `--exclude directory` sur `ec2-bundle-vol` pour éviter tout répertoire et sous-répertoire contenant des informations secrètes que vous ne souhaiteriez pas inclure dans votre regroupement. Excluez notamment toutes les paires de clés publiques/privées SSH appartenant à l'utilisateur, et les fichiers SSH `authorized_keys` lorsque vous créez un bundle de l'image. Les AMI publiques Amazon stockent ces éléments dans `/root/.ssh` pour l'utilisateur `root` et dans `/home/user_name/.ssh/` pour les utilisateurs réguliers. Pour plus d'informations, consultez [ec2-bundle-vol](#).
- Supprimez toujours l'historique shell avant la création d'un bundle. Si vous essayez de réaliser plusieurs téléchargements de regroupement dans une même AMI, l'historique shell contient votre clé d'accès. L'exemple ci-après devrait être la dernière commande que vous avez exécutée avant de créer un bundle depuis l'instance.

```
[ec2-user ~]$ shred -u ~/.*history
```

Warning

Les limites de **shred** décrites dans l'avertissement ci-dessus s'appliquent également ici. Ayez à l'esprit que `bash` inscrit l'historique de la session en cours sur le disque au moment de quitter. Si vous vous déconnectez de votre instance après avoir supprimé `~/.bash_history` et si vous vous reconnectez ensuite, vous constaterez que `~/.bash_history` a été recréé et contient toutes les commandes que vous avez exécutées durant votre session précédente.

D'autres programmes en dehors de `bash` inscrivent les historiques sur le disque. Soyez prudent et retirez ou excluez tous les fichiers et répertoires dot superflus.

- La création d'une offre groupée pour une instance en cours d'exécution nécessite votre clé privée et un certificat X.509. Mettez ces éléments et toutes les autres informations d'identification dans un endroit qui n'est pas regroupé (comme par exemple le stockage d'instances).

AMI payantes

Une AMI payante est une AMI mise en vente dans le AWS Marketplace. AWS Marketplace Il s'agit d'une boutique en ligne où vous pouvez acheter des logiciels qui s' AWS exécutent, y compris des AMI que vous pouvez utiliser pour lancer votre instance EC2. Les AWS Marketplace AMI sont organisées en catégories, telles que les outils de développement, pour vous permettre de trouver

des produits adaptés à vos besoins. Pour plus d'informations AWS Marketplace, consultez le [AWS Marketplace](#) site Web.

Vous pouvez acheter des AMI AWS Marketplace auprès d'un tiers, y compris des AMI associées à des contrats de service auprès d'organisations telles que Red Hat. Vous pouvez également créer une AMI et la vendre AWS Marketplace à d'autres utilisateurs d'Amazon EC2. La création d'une AMI sûre, sécurisée et utilisable à des fins d'utilisation publique est un processus relativement simple, à condition que vous respectiez quelques consignes simples. Pour plus d'informations sur la création et l'utilisation d'AMI partagées, consultez [AMI partagées](#).

Le lancement d'une instance à partir d'une AMI payante est identique au lancement d'une instance à partir de n'importe quelle AMI. Aucun paramètre supplémentaire n'est obligatoire. L'instance est facturée selon les tarifs définis par le propriétaire de l'AMI, ainsi que les frais d'utilisation standard pour les services Web associés, par exemple le taux horaire pour l'exécution d'un type d'instance m5.small dans Amazon EC2. Des taxes supplémentaires peuvent également être appliquées. Le propriétaire de l'AMI payante peut confirmer si une instance spécifique a été lancée à l'aide de cette AMI payante.

Important

Amazon DevPay n'accepte plus de nouveaux vendeurs ni de nouveaux produits. AWS Marketplace est désormais la plateforme de commerce électronique unique et unifiée pour la vente de logiciels et de services via AWS. Pour plus d'informations sur le déploiement et la vente de logiciels depuis AWS Marketplace, consultez [Selling in AWS Marketplace](#). AWS Marketplace prend en charge les AMI soutenues par Amazon EBS.

Table des matières

- [Vendre votre AMI](#)
- [Rechercher une AMI payante](#)
- [Acheter une AMI payante](#)
- [Obtenir le code produit pour votre instance](#)
- [Utiliser le support payant](#)
- [Factures pour les AMI payantes et supportées](#)
- [Gérez vos AWS Marketplace abonnements](#)

Vendre votre AMI

Vous pouvez vendre votre AMI en utilisant AWS Marketplace. AWS Marketplace propose une expérience d'achat organisée. En outre, il prend AWS Marketplace également en charge AWS des fonctionnalités telles que les AMI basées sur Amazon EBS, les instances réservées et les instances ponctuelles.

Pour plus d'informations sur la manière de vendre votre AMI sur le AWS Marketplace, consultez [Selling in AWS Marketplace](#).

Rechercher une AMI payante

Vous pouvez rechercher les AMI disponibles à l'achat de différentes façons. Par exemple, vous pouvez utiliser [AWS Marketplace](#), la console Amazon EC2 ou la ligne de commande. Les développeurs peuvent également vous avertir eux-mêmes de la disponibilité d'AMI payantes.

Rechercher une AMI payante à l'aide de la console

Pour rechercher une AMI payante à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Choisissez Images publiques comme premier filtre.
4. Dans la barre de recherche, sélectionnez Owner alias (Alias du propriétaire), puis =, et ensuite aws-marketplace.
5. Si vous connaissez le code produit, choisissez Code Produit, puis =, et entrez ensuite le code produit.

Trouvez une AMI payante à l'aide de AWS Marketplace

Pour trouver une AMI payante à l'aide de AWS Marketplace

1. Ouvrir [AWS Marketplace](#).
2. Saisissez le nom du système d'exploitation dans le champ de recherche, puis choisissez le bouton de recherche (loupe).
3. Pour affiner la recherche, utilisez l'une des catégories ou l'un des filtres.
4. Chaque produit est identifié par son type de produit : AMI ou Software as a Service.

Trouvez une AMI payante à l'aide du AWS CLI

Vous pouvez rechercher une AMI payante à l'aide de la commande [describe-images](#) suivante (AWS CLI).

```
aws ec2 describe-images
  --owners aws-marketplace
```

Cette commande renvoie un grand nombre d'informations qui décrivent chaque AMI, y compris le code produit d'une AMI payante. Le résultat de `describe-images` comprend une entrée pour le code produit, illustrée ici :

```
"ProductCodes": [
  {
    "ProductCodeId": "product_code",
    "ProductCodeType": "marketplace"
  }
],
```

Si vous connaissez le code produit, vous pouvez filtrer les résultats par code produit. Cet exemple renvoie l'AMI la plus récente ayant le code produit spécifié.

```
aws ec2 describe-images
  --owners aws-marketplace \
  --filters "Name=product-code,Values=product_code" \
  --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

Trouvez une AMI payante à l'aide des outils pour Windows PowerShell

Vous pouvez trouver une AMI payante à l'aide de la [Get-EC2Image](#) commande suivante.

```
PS C:\> Get-EC2Image -Owner aws-marketplace
```

La sortie pour une AMI payante comprend le code produit.

```
ProductCodeId      ProductCodeType
-----
product_code      marketplace
```

Si vous connaissez le code produit, vous pouvez filtrer les résultats par code produit. Cet exemple renvoie l'AMI la plus récente ayant le code produit spécifié.

```
PS C:\> (Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-code";"Value"="product_code"} | sort CreationDate -Descending | Select-Object -First 1).ImageId
```

Acheter une AMI payante

Vous devez vous inscrire à (acheter) une AMI payante avant de pouvoir lancer une instance à l'aide de l'AMI.

Généralement, le vendeur d'une AMI payante vous présente les informations relatives à l'AMI, notamment le tarif et un lien auquel vous accédez pour l'acheter. Lorsque vous cliquez sur le lien, vous êtes d'abord invité à vous connecter AWS, puis vous pouvez acheter l'AMI.

Acheter une AMI payante à l'aide de la console

Vous pouvez acheter une AMI payante à l'aide de l'assistant de lancement Amazon EC2. Pour plus d'informations, consultez [Lancer une AWS Marketplace instance](#).

Abonnez-vous à un produit en utilisant AWS Marketplace

Pour utiliser le AWS Marketplace, vous devez avoir un AWS compte. Pour lancer des instances à partir de AWS Marketplace produits, vous devez être inscrit pour utiliser le service Amazon EC2 et vous devez être abonné au produit à partir duquel vous souhaitez lancer l'instance. Vous pouvez vous abonner aux produits dans AWS Marketplace de deux façons :

- AWS Marketplace site Web : vous pouvez lancer rapidement des logiciels préconfigurés grâce à la fonction de déploiement en 1 clic.
- Assistant de lancement Amazon EC2 : vous pouvez rechercher une AMI et lancer une instance directement à partir de l'assistant. Pour plus d'informations, consultez [Lancer une AWS Marketplace instance](#).

Obtenir le code produit pour votre instance

Vous pouvez récupérer le code AWS Marketplace produit de votre instance à l'aide de ses métadonnées. Si l'instance comporte un code produit, Amazon EC2 le renvoie. Pour obtenir plus

d'informations sur la récupération des métadonnées, consultez [Récupérer des métadonnées d'instance](#).

Pour récupérer un code produit, utilisez la commande correspondant au système d'exploitation de votre instance.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/product-codes
```

Utiliser le support payant

Amazon EC2 permet également aux développeurs d'offrir un support pour les logiciels (ou AMI dérivées). Les développeurs peuvent créer des produits de support que vous pouvez utiliser en vous y inscrivant. Pendant le processus d'inscription au produit de support, le développeur vous fournit un code produit, que vous devez ensuite associer à votre propre AMI. Le développeur est ainsi en mesure de confirmer que votre instance peut bénéficier du support. Cela garantit également que, lorsque vous exécutez des instances du produit, le tarif appliqué correspond aux conditions définies pour le produit par le développeur.

Important

Vous ne pouvez pas utiliser un produit de support avec les instances réservées. Le tarif appliqué est toujours défini par le vendeur du produit de support.

Pour associer un code produit à votre AMI, utilisez l'une des commandes suivantes, dans lesquelles `ami_id` est l'ID de l'AMI et `product_code` est le code produit :

- [modify-image-attribute](#) (AWS CLI)

```
aws ec2 modify-image-attribute --image-id ami_id --product-codes "product_code"
```

- [Edit-EC2ImageAttribute](#) (AWS Tools for Windows PowerShell)

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami_id -ProductCode product_code
```

Une fois que vous avez défini l'attribut du code produit, il ne peut pas être modifié ni supprimé.

Factures pour les AMI payantes et supportées

A la fin de chaque mois, vous recevez un e-mail indiquant le montant prélevé sur votre carte de paiement pour l'utilisation des AMI payantes ou supportées au cours du mois. Cette facture est différente de votre facture Amazon EC2 habituelle. Pour plus d'informations, consultez la section [Paiement des produits](#) dans le AWS Marketplace Guide de l'acheteur.

Gérez vos AWS Marketplace abonnements

Sur le AWS Marketplace site Web, vous pouvez vérifier les détails de votre abonnement, consulter les instructions d'utilisation du fournisseur, gérer vos abonnements, etc.

Pour vérifier les informations concernant votre abonnement

1. Connectez-vous à [AWS Marketplace](#).
2. Choisissez Your Marketplace Account (Votre compte Marketplace).
3. Choisissez Manage your software subscriptions (Gérer vos abonnements logiciels).
4. Tous vos abonnements actuels sont répertoriés. Choisissez Usage Instructions (Instructions d'utilisation) pour consulter les instructions spécifiques à l'utilisation du produit, par exemple le nom d'utilisateur pour la connexion à votre instance en cours d'exécution.

Pour annuler un AWS Marketplace abonnement

1. Vérifiez que vous avez mis fin à toutes les instances en cours d'exécution à partir de l'abonnement.

- a. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
 - b. Dans le panneau de navigation, sélectionnez Instances.
 - c. Sélectionnez l'instance, choisissez État de l'instance, Résilier l'instance.
 - d. Choisissez Résilier lorsque vous êtes invité à confirmer.
2. Connectez-vous à [AWS Marketplace](#), puis choisissez Your Marketplace Account (Votre compte Marketplace) et Manage your software subscriptions (Gérer vos abonnements logiciels).
 3. Choisissez Cancel subscription (Annuler l'abonnement). Vous êtes invité à confirmer l'annulation.

 Note

Après avoir annulé votre abonnement, vous ne pouvez plus lancer d'instances à partir de cette AMI. Pour réutiliser cette AMI, vous devez vous y réabonner, soit sur le AWS Marketplace site Web, soit via l'assistant de lancement de la console Amazon EC2.

Cycle de vie de l'AMI

Vous pouvez créer vos propres AMI, les copier, les sauvegarder et les conserver jusqu'à ce que vous soyez prêt à les rendre obsolètes ou à annuler leur enregistrement.

Table des matières

- [Créer une AMI](#)
- [Modification d'une AMI](#)
- [Copier une AMI](#)
- [Stocker et restaurer une AMI à l'aide de S3](#)
- [Rendre obsolète une AMI](#)
- [Désactiver une AMI](#)
- [Archiver des instantanés d'AMI](#)
- [Désenregistrer \(supprimer\) une AMI](#)
- [Automatiser le cycle de vie des AMI basées sur EBS](#)

Créer une AMI

Vous pouvez créer des AMI Linux ou Windows sauvegardées par des volumes Amazon EBS. Vous pouvez également créer des AMI Linux soutenues par des volumes de stockage d'instance (les AMI Windows ne prennent pas en charge le stockage d'instance pour le périphérique racine). Vous pouvez également utiliser Windows Sysprep pour créer des AMI Windows.

Rubriques

- [Création d'une AMI basée sur Amazon EBS](#)
- [Créer une AMI Linux basée sur le stockage d'instance](#)
- [Création d'une AMI avec Windows Sysprep](#)

Création d'une AMI basée sur Amazon EBS

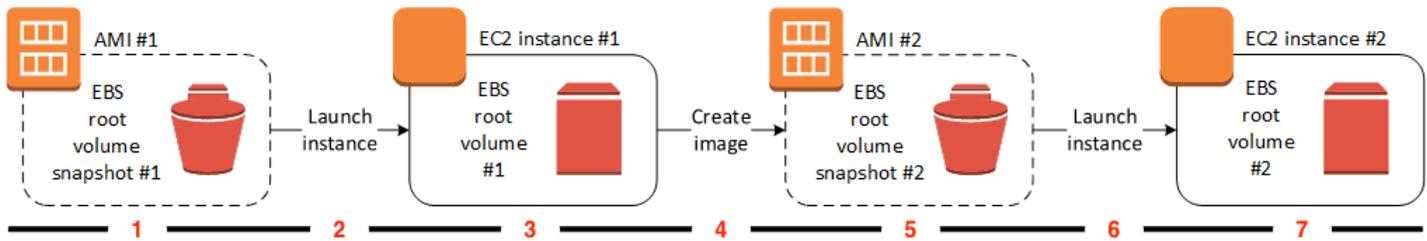
Pour créer une AMI basée sur Amazon EBS, commencez par une instance que vous avez lancée à partir d'une AMI existante basée sur Amazon EBS. Il peut s'agir d'une AMI que vous avez obtenue auprès du AWS Marketplace, d'une AMI que vous avez créée à l'[AWS Server Migration Service](#) aide de [VM Import/Export](#), ou de toute autre AMI accessible. Après avoir personnalisé l'instance pour répondre à vos besoins, créez et enregistrez une nouvelle AMI. Vous pouvez l'utiliser pour lancer de nouvelles instances avec ces personnalisations.

Les procédures décrites ci-dessous s'appliquent aux instances Amazon EC2 sauvegardées sur des volumes Amazon Elastic Block Store (Amazon EBS) chiffrés (notamment le volume racine) ainsi que pour les volumes non chiffrés.

Le processus de création d'une AMI est différent de celui des AMIs basées sur le stockage d'instances. Pour plus d'informations sur les différences entre les instances basées sur des volumes Amazon EBS et celles basées sur un stockage d'instances et les façons de déterminer le type de périphérique racine pour votre instance, consultez [Stockage pour le périphérique racine](#). Pour plus d'informations sur la création d'une AMI basée sur une instance store-backed, consultez. [Créer une AMI Linux basée sur le stockage d'instance](#)

Présentation de la création d'AMIs basées sur des volumes Amazon EBS

Le diagramme suivant résume le processus de création d'une AMI Amazon EBS à partir d'une instance EC2 en cours d'exécution : commencez avec une AMI existante, lancez une instance, personnalisez-la, créez une AMI à partir de celle-ci, puis lancez une instance de votre nouvelle AMI. Les chiffres du diagramme correspondent à ceux de la description qui suit.



1 – AMI n° 1 : commencer avec une AMI existante

Recherchez une AMI existante qui est similaire à l'AMI que vous souhaiteriez créer. Il peut s'agir d'une AMI que vous avez obtenue auprès du AWS Marketplace, d'une AMI que vous avez créée à l'[AWS Server Migration Service](#) aide de [VM Import/Export](#), ou de toute autre AMI accessible. Vous allez personnaliser cette AMI en fonction de vos besoins.

Dans le diagramme, EBS root volume snapshot #1 (Instantané du volume racine EBS n° 1) indique que l'AMI est une AMI Amazon EBS et que les informations sur le volume racine sont stockées dans cet instantané.

2 – Lancer une instance à partir d'une AMI existante

Pour configurer une AMI, vous devez lancer une instance à partir de l'AMI sur laquelle vous souhaitez baser votre nouvelle AMI, puis personnaliser l'instance (3 dans le diagramme). Vous allez ensuite créer une nouvelle AMI qui inclut les personnalisations (4 dans le diagramme).

3 – Instance EC2 n° 1 : Personnaliser l'instance

Connectez-vous à votre instance et personnalisez-la selon vos besoins. Votre nouvelle AMI inclura ces personnalisations.

Vous pouvez effectuer toutes les actions suivantes sur votre instance pour la personnaliser :

- Installer les logiciels et les applications
- Copier les données
- Réduire le temps de démarrage en supprimant les fichiers temporaires et en défragmentant le disque dur
- Attacher des volumes EBS supplémentaires

4 – Créer une image

Lorsque vous créez une AMI à partir d'une instance, Amazon EC2 désactive l'instance avant de créer l'AMI pour s'assurer que tout le contenu de l'instance est arrêté et dans un état cohérent pendant le processus de création. Si vous êtes sûr que votre instance est dans un état cohérent approprié pour la création d'une AMI, vous pouvez indiquer à Amazon EC2 de ne pas procéder à

la mise hors tension et redémarrer l'instance. Certains systèmes de fichiers, comme XFS, peuvent bloquer et débloquer l'activité ce qui sécurise la création de l'image sans redémarrer l'instance.

Pendant le processus de création d'AMI, Amazon EC2 crée des instantanés du volume racine de votre instance et de tout autre volume EBS attaché à cette dernière. Les instantanés vous sont facturés jusqu'à ce que vous [annuliez l'inscription de l'AMI](#) et que vous les supprimiez. Si un volume attaché à l'instance est chiffré, la nouvelle AMI se lance uniquement avec succès sur les instances qui prennent en charge le chiffrement Amazon EBS.

En fonction de la taille des volumes, le processus de création de l'AMI peut prendre quelques minutes pour se terminer (parfois jusqu'à 24 heures). Il se peut que la création d'instantanés de vos volumes avant de créer votre AMI vous paraisse plus efficace. De cette façon, seuls de petits instantanés incrémentiels doivent être formés lorsque l'AMI est créée, et le processus se termine plus rapidement (la durée totale de la création des instantanés reste la même).

5 – AMI n° 2 : Nouvelle AMI

Une fois le processus terminé, vous disposez d'une nouvelle AMI et d'un instantané (instantané n° 2) créés à partir du volume racine de l'instance. Si vous avez ajouté des volumes EBS ou de stockage d'instance à l'instance en plus du volume du périphérique racine, le mappage de périphérique de stockage en mode bloc pour la nouvelle AMI contient des informations pour ces volumes.

Amazon EC2 enregistre automatiquement l'AMI pour vous.

6 – Lancer une nouvelle instance à partir de la nouvelle AMI

Vous pouvez utiliser la nouvelle AMI pour lancer une instance.

7 – Instance EC2 n° 2 : Nouvelle instance

Lorsque vous lancez une instance à l'aide de la nouvelle AMI, Amazon EC2 crée un nouveau volume EBS pour le volume racine de l'instance en utilisant l'instantané. Si vous avez ajouté des volumes EBS ou de stockage d'instance lorsque vous avez personnalisé l'instance, le mappage de périphérique de stockage en mode bloc pour la nouvelle AMI contient des informations pour ces volumes, et les mappages de périphérique de stockage en mode bloc pour les instances que vous lancez depuis la nouvelle AMI contiennent automatiquement des informations pour ces volumes. Les volumes de stockage d'instance spécifiés dans le mappage de périphérique de stockage en mode bloc pour la nouvelle instance sont nouveaux et ne contiennent aucune donnée des volumes de stockage d'instance de l'instance que vous avez utilisée pour créer l'AMI. Les données sur les volumes EBS persistent. Pour plus d'informations, consultez [Mappages de périphériques de stockage en mode bloc](#).

Lorsque vous créez une instance à partir d'une AMI basée sur EBS, vous devez initialiser son volume racine et tout stockage EBS supplémentaire avant de la mettre en production. Pour plus d'informations, consultez [Initialiser les volumes Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Création d'une AMI à partir d'une instance

Vous pouvez créer une AMI à l'aide de la ligne de commande AWS Management Console ou de la ligne de commande.

Console

Pour créer une AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance à partir de laquelle vous souhaitez créer l'AMI, puis choisissez Actions, Image and templates (Image et modèles), et enfin Create image (Créer une image).

Tip

Si cette option est désactivée, votre instance n'est pas une instance basée sur Amazon EBS.

4. Sur la page Create image (Créer une image), spécifiez les informations suivantes :
 - a. Pour Image name (Nom de l'image), saisissez un nom unique pour l'image de 127 caractères au maximum.
 - b. Pour Image description (Description de l'image), saisissez une description facultative de l'image de 255 caractères au maximum.
 - c. Pour No reboot (Pas de redémarrage), laissez la case Enable (Activer) décochée (valeur par défaut) ou sélectionnez-la.
 - Si la case Activer pour Pas de redémarrage est décochée lorsqu'Amazon EC2 crée l'AMI, il redémarre l'instance afin de pouvoir prendre des instantanés des volumes attachés pendant que les données sont au repos, afin de garantir un état cohérent.
 - Si la case Activer pour Pas de redémarrage est cochée lorsque Amazon EC2 crée l'AMI, il n'arrête ni ne redémarre l'instance.

⚠ Warning

Si vous choisissez d'activer l'option No reboot, nous ne pouvons pas garantir l'intégrité du système de fichiers de l'image créée.

- d. Volumes d'instance : vous pouvez modifier le volume racine et ajouter des volumes Amazon EBS et des volumes de stockage d'instances supplémentaires, comme suit :
 - i. Le volume racine est défini dans la première ligne.
 - Pour modifier la taille du volume racine, saisissez la valeur requise dans Size (Taille).
 - Si vous sélectionnez Delete on termination (Supprimer à la résiliation), lorsque vous résiliez l'instance créée à partir de cette AMI, le volume EBS est supprimé. Si vous désélectionnez Delete on termination (Supprimer à la résiliation), lorsque vous résiliez l'instance, le volume EBS n'est pas supprimé. Pour plus d'informations, consultez [Conservation des données lors de la résiliation d'une instance](#).
 - ii. Pour ajouter un volume EBS, sélectionnez Add volume (Ajouter un volume) (ce qui ajoute une nouvelle ligne). Pour Type de stockage, sélectionnez EBS et remplissez les champs de la ligne. Lorsque vous lancez une instance à partir de votre nouvelle AMI, des volumes supplémentaires sont automatiquement attachés à l'instance. Les volumes vides doivent être formatés et montés. Les volumes basés sur un instantané doivent être montés.
 - iii. Pour ajouter un volume de stockage d'instance, consultez [Ajouter des volumes de stockage d'instance à une AMI](#). Lorsque vous lancez une instance à partir de votre nouvelle AMI, les volumes supplémentaires sont automatiquement initialisés et montés. Ces volumes ne contiennent pas les données des volumes de stockage d'instance de l'instance en cours d'exécution sur laquelle vous avez basé votre AMI.
- e. Balises : vous pouvez baliser l'AMI et les instantanés avec les mêmes balises ou avec des balises différentes.
 - Pour baliser l'AMI et les instantanés avec les mêmes balises, sélectionnez Tag image and snapshots together (Baliser l'image et les instantanés ensemble). Les mêmes balises sont appliquées à l'AMI et à chaque instantané créé.

- Pour baliser l'AMI et les instantanés avec des balises différentes, sélectionnez `Tag image and snapshots separately` (Baliser l'image et les instantanés séparément). Différentes balises sont appliquées à l'AMI et aux instantanés créés. Cependant, tous les instantanés obtiennent les mêmes balises ; vous ne pouvez pas baliser chaque instantané avec une balise différente.

(Facultatif) Pour ajouter une balise, sélectionnez `Add tag` (Ajouter une balise) et saisissez la clé et la valeur de la balise. Répétez l'opération pour chaque étiquette.

- f. Lorsque vous êtes prêt à créer votre AMI, choisissez `Create image` (Créer une image).
5. Pour afficher le statut de votre AMI pendant sa création :
 - a. Dans le panneau de navigation, sélectionnez `AMI`.
 - b. Définissez le filtre sur `Owned by me` (M'appartenant) et recherchez votre AMI dans la liste.

À l'origine, le statut est `pending` mais il doit être remplacé par `available` après quelques minutes.

6. (Facultatif) Pour afficher l'instantané qui a été créé pour la nouvelle AMI :
 - a. Notez l'ID de votre AMI que vous avez localisé à l'étape précédente.
 - b. Dans le panneau de navigation, choisissez `Snapshots` (Instantanés).
 - c. Définissez le filtre sur `Owned by me` (M'appartenant), puis recherchez l'instantané contenant le nouvel ID d'AMI dans la colonne `Description`.

Lorsque vous lancez une instance à partir de cette AMI, Amazon EC2 cet instantané pour créer son volume du périphérique racine.

AWS CLI

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [create-image](#) (AWS CLI)
- [New-EC2Image](#) (AWS Tools for Windows PowerShell)

Créer une AMI Linux à partir d'un instantané

Si vous avez un instantané du volume du périphérique racine d'une instance, vous pouvez créer une AMI Linux à partir de cet instantané à l'aide de la ligne de commande AWS Management Console ou. Cette fonctionnalité n'est actuellement pas disponible pour les instances Windows.

Console

Pour créer une AMI à partir d'un instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané à partir duquel créer l'AMI, puis choisissez Actions, Create image from snapshot (Créer une image à partir d'un instantané).
4. Sur la page Créer une image à partir d'un instantané, spécifiez les informations suivantes :
 - a. Pour Image name (Nom de l'image), saisissez un nom descriptif pour l'image.
 - b. Pour Description, saisissez une brève description pour l'image.
 - c. Pour Architecture, choisissez l'architecture de l'image. Choisissez i386 pour 32 bits, x86_64 pour 64 bits, arm64 pour ARM 64 bits ou x86_64 pour macOS 64 bits.
 - d. Pour Root device name (Nom du périphérique racine), saisissez le nom du périphérique à utiliser pour le volume du périphérique racine. Pour plus d'informations, consultez [Noms des appareils sur les instances Amazon EC2](#).
 - e. Pour Virtualization type (Type de virtualisation), choisissez le type de virtualisation à utiliser par les instances lancées à partir de cette AMI. Pour plus d'informations, consultez [Types de virtualisation AMI](#).
 - f. (Pour la virtualisation paravirtuelle uniquement) Pour Kernel ID (ID du noyau), sélectionnez le noyau du système d'exploitation pour l'image. Si vous utilisez un instantané du volume du périphérique racine d'une instance, sélectionnez le même ID du noyau que celui de l'instance d'origine. Si vous avez un doute, utilisez le noyau par défaut.
 - g. (Pour la virtualisation paravirtuelle uniquement) Pour RAM disk ID (ID de disque RAM), sélectionnez le disque RAM pour l'image. Si vous sélectionnez un noyau spécifique, vous devrez peut-être sélectionner un disque RAM spécifique avec les pilotes qui le prennent en charge.

- h. Pour le mode de démarrage, choisissez le mode de démarrage de l'image ou choisissez Utiliser par défaut afin que, lorsqu'une instance est lancée avec cette AMI, elle démarre avec le mode de démarrage pris en charge par le type d'instance. Pour plus d'informations, consultez [Définir le mode de démarrage d'une AMI](#).
- i. (Facultatif) Sous Bloquer les mappages de périphériques, personnalisez le volume racine et ajoutez des volumes de données supplémentaires.

Pour chaque volume, vous pouvez spécifier la taille, le type, les caractéristiques de performance, le comportement de la suppression lors de la résiliation et le statut de chiffrement. Pour le volume racine, la taille ne peut pas être inférieure à celle de l'instantané. Pour le type de volume, le stockage SSD à usage général gp3 est sélectionné par défaut.

- j. (Facultatif) Sous Balises, vous pouvez ajouter une ou plusieurs balises à la nouvelle AMI. (Facultatif) Pour ajouter une balise, sélectionnez Add tag (Ajouter une balise) et saisissez la clé et la valeur de la balise. Répétez l'opération pour chaque étiquette.
- k. Lorsque vous êtes prêt à créer votre AMI, choisissez Create image (Créer une image).

AWS CLI

Pour créer une AMI à partir d'un instantané en utilisant la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel [Accès à Amazon EC2](#).

- [image de registre \(CLI\)AWS](#)
- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

Lancez une instance à partir d'une AMI que vous avez créée

Vous pouvez lancer une instance à partir d'une AMI que vous avez créée à partir d'une instance ou d'un instantané.

Pour lancer une instance à partir de votre AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Images, choisissez AMIs (AMI).
3. Définissez le filtre sur Owned by me (M'appartenant) et sélectionnez votre AMI.

4. Choisissez Lancer une instance à partir d'une AMI.
5. Acceptez les valeurs par défaut ou spécifiez des valeurs personnalisées dans l'assistant de lancement d'instance. Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Créer une AMI Linux basée sur le stockage d'instance

L'AMI que vous spécifiez au lancement de votre instance détermine le type de volume du périphérique racine.

Pour créer une AMI Linux basée sur le stockage d'instance, démarrez à partir d'une instance que vous avez lancée depuis une AMI Linux basée sur le stockage d'instance existante. Après avoir personnalisé l'instance pour répondre à vos besoins, créez un bundle du volume et inscrivez une nouvelle AMI que vous pouvez utiliser pour lancer de nouvelles instances avec ces personnalisations.

Vous ne pouvez pas créer d'AMI Windows basée sur un magasin d'instances, car les AMI Windows ne prennent pas en charge le stockage d'instance pour le périphérique racine.

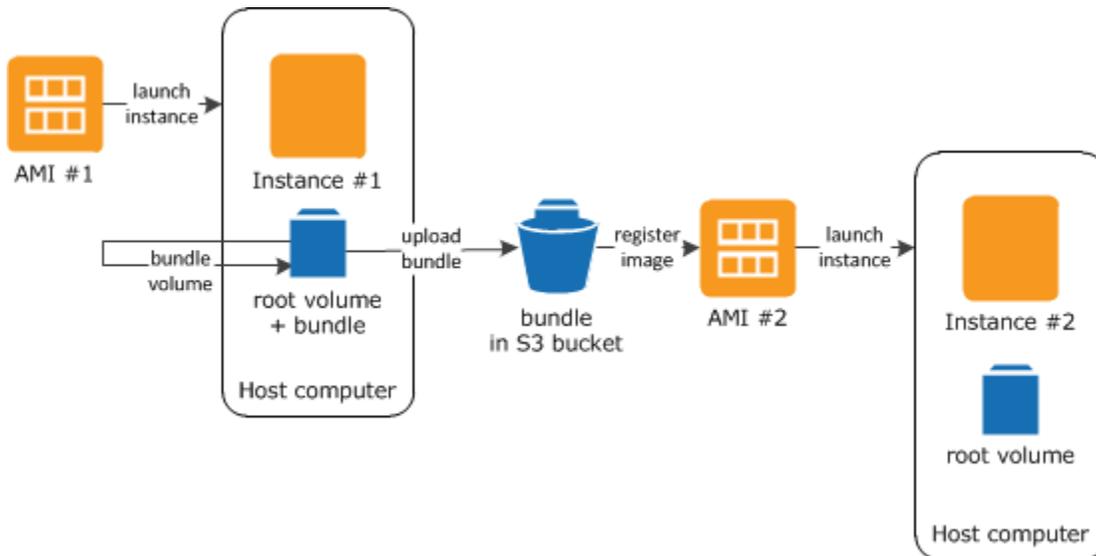
Important

Seuls les types d'instance suivants prennent en charge un volume de stockage d'instance en tant que périphérique racine : C1, C3, D2, I2, M1, M2, M3, R3 et X1.

Le processus de création de l'AMI est différent de celui des AMI basées sur les volumes Amazon EBS. Pour plus d'informations sur les différences entre les instances basées sur des volumes Amazon EBS et celles basées sur un stockage d'instance et les façons de déterminer le type de périphérique racine pour votre instance, consultez [Stockage pour le périphérique racine](#). Si vous devez créer une AMI basée sur Amazon EBS, consultez. [Création d'une AMI basée sur Amazon EBS](#)

Présentation du processus de création des AMI basées sur le stockage d'instance

Le graphique suivant résume le processus de création d'une AMI à partir d'une instance basée sur le stockage d'instance.



Tout d'abord, lancez une instance depuis une AMI qui est similaire à l'AMI que vous souhaiteriez créer. Vous pouvez vous connecter à votre instance et la personnaliser. Lorsque l'instance est configurée comme vous le voulez, vous pouvez en créer un bundle. Le processus de création d'un bundle peut prendre plusieurs minutes. Après la fin du processus, vous avez un groupe qui se compose d'un manifeste d'image (`image.manifest.xml`) et de fichiers (`image.part.xx`) contenant un modèle pour le volume racine. Ensuite, vous chargez le bundle dans votre compartiment Amazon S3, puis vous inscrivez votre AMI.

Note

Afin de charger des objets vers un compartiment S3 pour votre AMI Linux basée sur le stockage d'instances, les listes de contrôle d'accès doivent être activées pour le compartiment. Sinon, Amazon EC2 ne sera pas en mesure de définir des listes ACL sur les objets à charger. Si votre compartiment de destination utilise le paramètre appliqué par le propriétaire du compartiment pour la propriété de l'objet S3 (S3 Object Ownership), cela ne fonctionnera pas car les listes de contrôle d'accès sont désactivées. Pour plus d'informations, consultez la section [Contrôle de la propriété des objets chargés à l'aide de la propriété de l'objet S3](#).

Lorsque vous lancez une instance à l'aide de la nouvelle AMI, nous créons le volume racine pour l'instance avec le bundle que vous avez chargé sur Amazon S3. L'espace de stockage utilisé par le bundle dans Amazon S3 entraîne des frais sur votre compte jusqu'à ce que vous le supprimiez. Pour plus d'informations, consultez [Désenregistrer \(supprimer\) une AMI](#).

Si vous ajoutez des volumes de stockage d'instance à votre instance en plus de votre volume du périphérique racine, le mappage de périphérique de stockage en mode bloc pour la nouvelle AMI contient des informations pour ces volumes et les mappages de périphérique de stockage en mode bloc pour les instances que vous lancez depuis la nouvelle AMI contient automatiquement des informations pour ces volumes. Pour plus d'informations, consultez [Mappages de périphériques de stockage en mode bloc](#).

Prérequis

Avant de créer un AMI, vous devez terminer les tâches suivantes :

- Installez les outils AMI. Pour plus d'informations, consultez [Configurer les outils AMI](#).
- Installez le AWS CLI. Pour plus d'informations, consultez la page [Préparation de l'installation de l'AWS Command Line Interface](#).
- Assurez-vous d'avoir un compartiment S3 pour la solution groupée et que les ACL sont activées dans votre compartiment. Pour plus d'informations sur la configuration des ACL, consultez [Configuration des listes ACL](#).
 - Pour créer un compartiment S3 à l'aide de AWS Management Console, ouvrez la console Amazon S3 à l'[adresse https://console.aws.amazon.com/s3/](https://console.aws.amazon.com/s3/) et choisissez Create Bucket.
 - Pour créer un compartiment S3 avec le AWS CLI, vous pouvez utiliser la commande `mb`. Si la version installée des outils AMI est la version 1.5.18 ou toute autre version ultérieure, vous pouvez également utiliser la commande `ec2-upload-bundle` pour créer le compartiment S3. Pour plus d'informations, consultez [ec2-upload-bundle](#).
- Assurez-vous d'avoir votre identifiant de AWS compte. Pour plus d'informations, voir [Afficher les Compte AWS identifiants](#) dans le Guide de référence de gestion des AWS comptes.
- Assurez-vous de disposer des informations d'identification nécessaires pour utiliser l' AWS CLI. Pour plus d'informations, consultez la section [Meilleures pratiques relatives aux AWS comptes](#) dans le Guide de AWS Account Management référence.
- Assurez-vous d'avoir un certificat X.509 et la clé privée correspondante.
 - Si vous avez besoin créer un certificat X.509, consultez la section [Gérer les certificats de signature](#). Le certificat X.509 et la clé privée sont utilisés pour chiffrer et déchiffrer votre AMI.
 - [Chine (Pékin)] Utilisez le certificat `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem`.
 - [AWS GovCloud (US-West)] Utilisez le `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem` certificat.

- Connectez-vous à votre instance et personnalisez-la. Par exemple, vous pouvez installer des logiciels et des applications, copier des données, supprimer des fichiers temporaires et modifier la configuration Linux.

Tâches

- [Configurer les outils AMI](#)
- [Créer une AMI à partir d'une instance Amazon Linux basée sur un stockage d'instance](#)
- [Créer une AMI à partir d'une instance Ubuntu basée sur un stockage d'instance](#)
- [Convertir une AMI basée sur un stockage d'instance en AMI basée sur des volumes Amazon EBS](#)

Configurer les outils AMI

Vous pouvez utiliser les outils AMI pour créer et gérer des AMIs Linux basées sur le stockage d'instance. Pour utiliser ces outils, vous devez les installer sur votre instance Linux. Les outils AMI sont disponibles sous forme de fichiers RPM et .zip pour les distributions Linux ne prenant pas en charge RPM.

Pour installer les outils AMI à l'aide d'un fichier RPM

1. Installez Ruby en utilisant le gestionnaire de package pour votre distribution de Linux, par exemple yum. Exemples :

```
[ec2-user ~]$ sudo yum install -y ruby
```

2. Téléchargez le fichier RPM à l'aide d'un outil tel que wget ou curl. Exemples :

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. Vérifiez la signature du fichier RPM en utilisant la commande suivante :

```
[ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
```

La commande ci-dessus doit indiquer que les hachages SHA1 et MD5 du fichier sont OK. Si la commande indique que les hachages sont NOT OK, utilisez la commande suivante pour afficher les hachages SHA1 et MD5 d'en-tête du fichier :

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

Ensuite, comparez les hachages SHA1 et MD5 d'en-tête du fichier avec les hachages des outils d'AMI vérifiés suivants pour confirmer l'authenticité du fichier :

- SHA1 d'en-tête : a1f662d6f25f69871104e6a62187fa4df508f880
- MD5 : 9faff05258064e2f7909b66142de6782

Si les hachages SHA1 et MD5 d'en-tête du fichier correspondent aux hachages des outils d'AMI vérifiés, passez à l'étape suivante.

4. Installez le fichier RPM à l'aide de la commande suivante:

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. Vérifiez l'installation de vos outils AMI avec la commande [ec2-ami-tools-version](#).

```
[ec2-user ~]$ ec2-ami-tools-version
```

Note

Si vous recevez une erreur de chargement du type « impossible de charger ce fichier -- ec2/amitools/version (LoadError) », passez à l'étape suivante pour ajouter l'emplacement de l'installation de vos outils AMI à votre chemin. RUBYLIB

6. (Facultatif) Si vous avez reçu une erreur à l'étape précédente, ajoutez l'emplacement d'installation de vos outils AMI pour votre chemin d'accès RUBYLIB.
 - a. Exécutez la commande suivante afin de déterminer les chemins à ajouter.

```
[ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
/usr/lib/ruby/site_ruby/ec2/amitools/version.rb
/usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
```

Dans l'exemple ci-dessus, le fichier manquant à partir de l'erreur de chargement précédente est situé aux emplacements `/usr/lib/ruby/site_ruby` et `/usr/lib64/ruby/site_ruby`.

- b. Ajoutez les emplacements à partir de l'étape précédente pour votre chemin d'accès.

RUBYLIB

```
[ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/site_ruby
```

- c. Vérifiez l'installation de vos outils AMI avec la commande [ec2-ami-tools-version](#).

```
[ec2-user ~]$ ec2-ami-tools-version
```

Pour installer les outils AMI à l'aide du fichier .zip

1. Installez Ruby et décompressez en utilisant le gestionnaire de package pour votre distribution de Linux, comme apt-get. Exemples :

```
[ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. Téléchargez le fichier .zip à l'aide d'un outil tel que wget ou curl. Exemples :

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. Décompressez les fichiers dans un répertoire d'installation approprié, tel que /usr/local/ec2.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

Notez que le fichier .zip contient un dossier ec2-ami-tools-x.x.x, où x.x.x correspond au numéro de version des outils (par exemple, ec2-ami-tools-1.5.7).

4. Définissez la variable d'environnement EC2_AMIT00L_HOME sur le répertoire d'installation des outils. Exemples :

```
[ec2-user ~]$ export EC2_AMIT00L_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Ajoutez les outils à votre variable d'environnement PATH. Exemples :

```
[ec2-user ~]$ export PATH=$EC2_AMIT00L_HOME/bin:$PATH
```

6. Vous pouvez vérifier l'installation de vos outils AMI avec la commande [ec2-ami-tools-version](#).

```
[ec2-user ~]$ ec2-ami-tools-version
```

Gérer les certificats de signature

Certaines commandes dans les outils AMI nécessitent un certificat de signature (également appelé certificat X.509). Vous devez créer le certificat, puis le télécharger sur AWS. Par exemple, vous pouvez utiliser un outil tiers tel que OpenSSL pour créer le certificat.

Pour créer un certificat de signature

1. Installer et configurer OpenSSL.
2. Créez une clé privée à l'aide de la commande `openssl genrsa` et enregistrez la sortie dans un fichier `.pem`. Nous vous recommandons de créer une clé RSA 2048 bits ou 4096 bits.

```
openssl genrsa 2048 > private-key.pem
```

3. Générez un certificat à l'aide de la commande `openssl req`.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -  
out certificate.pem
```

Pour télécharger le certificat sur AWS, utilisez la commande [upload-signing-certificate](#).

```
aws iam upload-signing-certificate --user-name user-name --certificate-body  
file://path/to/certificate.pem
```

Pour afficher les certificats d'un utilisateur, utilisez la commande [list-signing-certificates](#) :

```
aws iam list-signing-certificates --user-name user-name
```

Pour désactiver ou réactiver un certificat de signature pour un utilisateur, utilisez la commande [update-signing-certificate](#). La commande suivante désactive le certificat :

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX704BEXAMPLE --  
status Inactive --user-name user-name
```

Pour supprimer un certificat, utilisez la commande [delete-signing-certificate](#) :

```
aws iam delete-signing-certificate --user-name user-name --certificate-  
id OFHPLP4ZULTHYPMSYEX704BEXAMPLE
```

Créer une AMI à partir d'une instance basée sur le stockage d'instance

Les procédures suivantes sont destinées à la création d'une AMI basée sur le stockage d'instance à partir d'une instance basée sur le stockage d'instance. Avant de commencer, prenez connaissance des [prérequis](#).

Rubriques

- [Créer une AMI à partir d'une instance Amazon Linux basée sur un stockage d'instance](#)
- [Créer une AMI à partir d'une instance Ubuntu basée sur un stockage d'instance](#)

Créer une AMI à partir d'une instance Amazon Linux basée sur un stockage d'instance

Cette section décrit la création d'une AMI à partir d'une instance Amazon Linux. Il est possible que les procédures suivantes ne fonctionnent pas pour les instances exécutant d'autres distributions Linux. Pour les procédures spécifiques à Ubuntu, consultez [Créer une AMI à partir d'une instance Ubuntu basée sur un stockage d'instance](#).

Pour se préparer à utiliser les outils AMI (instances HVM uniquement)

1. Les outils AMI ont besoin de GRUB Legacy pour démarrer correctement. Utilisez la commande suivante pour installer GRUB :

```
[ec2-user ~]$ sudo yum install -y grub
```

2. Installez les packages de gestion de partition à l'aide de la commande suivante :

```
[ec2-user ~]$ sudo yum install -y gdisk kpartx parted
```

Pour créer une AMI à partir d'une instance Amazon Linux basée sur un stockage d'instance

Cette procédure part du principe que vous avez respecté les prérequis dans [Prérequis](#).

Dans les commandes suivantes, remplacez chaque *espace réservé pour l'entrée utilisateur* par vos propres informations.

1. Chargez vos informations d'identification sur votre instance. Nous utilisons ces informations d'identification pour garantir que seuls vous et Amazon EC2 peuvent accéder à votre AMI.
 - a. Créez un répertoire temporaire sur votre instance pour vos informations d'identification en suivant ce qui suit :

```
[ec2-user ~]$ mkdir /tmp/cert
```

Ceci vous permet d'exclure vos informations d'identification de l'image créée.

- b. Copiez votre certificat X.509 et votre clé privée correspondante depuis votre ordinateur vers le répertoire `/tmp/cert` de votre instance en utilisant un outil de copie sécurisé tel que [scp](#). L'option `-i my-private-key.pem` de la commande `scp` suivante est la clé privée que vous utilisez pour vous connecter à votre instance avec SSH, et non la clé privée X.509. Exemples :

```
you@your_computer:~ $ scp -i my-private-key.pem /  
path/to/pk-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem /  
path/to/cert-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem ec2-  
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/  
pk-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem 100% 717 0.7KB/s 00:00  
cert-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem 100% 685 0.7KB/s 00:00
```

Sinon, étant donné qu'il s'agit de fichiers de texte brut, vous pouvez ouvrir le certificat et la clé dans un éditeur de texte et copier leur contenu dans de nouveaux fichiers dans le répertoire `/tmp/cert`.

2. Préparez le bundle à charger sur Amazon S3 en exécutant la commande [ec2-bundle-vol](#) depuis votre instance. Assurez-vous de spécifier l'option `-e` pour exclure le répertoire où vos informations d'identification sont stockées. Par défaut, la création d'un bundle exclut les fichiers qui peuvent contenir des informations sensibles. Ces fichiers incluent `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*`, `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` et `*/.bash_history`. Pour inclure tous ces fichiers, utilisez l'option `--no-filter`. Pour inclure certains de ces fichiers, utilisez l'option `--include`.

Important

Par défaut, le processus de création d'un bundle d'AMI génère un ensemble de fichiers compressés et chiffrés dans le répertoire `/tmp` qui représente le volume racine. Si vous

n'avez pas suffisamment d'espace disque libre dans `/tmp` pour stocker le groupe, vous devez spécifier un emplacement différent pour qu'il soit stocké avec l'option `-d /path/to/bundle/storage`. Certaines instances disposent d'un stockage éphémère installé `/mnt` ou `/media/ephemeral0` que vous pouvez utiliser, ou vous pouvez également créer, joindre et monter un nouveau volume Amazon (EBS) pour stocker le bundle. Pour plus d'informations, consultez la section [Créer un volume Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

- a. Vous devez exécuter la commande `ec2-bundle-vol` en tant que racine. Pour la plupart des commandes, vous pouvez utiliser `sudo` afin d'obtenir des autorisations d'un niveau élevé, mais dans ce cas, vous devriez exécuter `sudo -E su` pour conserver vos variables d'environnement.

```
[ec2-user ~]$ sudo -E su
```

Notez que l'invite de commande de Bash vous identifie maintenant en tant qu'utilisateur racine, et que le signe dollar a été remplacé par un hashtag, ce qui indique que vous êtes dans un shell racine :

```
[root ec2-user]#
```

- b. Pour créer le bundle AMI, exécutez la commande [ec2-bundle-vol](#) comme suit :

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --  
partition gpt
```

Note

Pour les régions de Chine (Pékin) et AWS GovCloud (ouest des États-Unis), utilisez le `--ec2cert` paramètre et spécifiez les certificats conformément aux [prérequis](#).

La création de l'image peut prendre quelques minutes. Lorsque cette commande se termine, le répertoire `/tmp` (ou votre répertoire personnalisé) contient le groupe (`image.manifest.xml`, ainsi que plusieurs fichiers `image.part.xx`).

- c. Quittez le shell racine.

```
[root ec2-user]# exit
```

3. (Facultatif) Pour ajouter davantage de volumes de stockage d'instance, modifiez les mappages de périphérique de stockage en mode bloc dans le fichier `image.manifest.xml` pour votre AMI. Pour plus d'informations, consultez [Mappages de périphériques de stockage en mode bloc](#).

- a. Créez une sauvegarde de votre fichier `image.manifest.xml`.

```
[ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

- b. Reformatez le fichier `image.manifest.xml` pour qu'il soit plus facile à lire et à modifier.

```
[ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/  
image.manifest.xml
```

- c. Modifiez les mappages de périphérique de stockage en mode bloc dans `image.manifest.xml` avec un éditeur de texte. L'exemple ci-dessous montre une nouvelle entrée pour le volume de stockage d'instance `ephemeral1`.

Note

Pour obtenir la liste des fichiers exclus, consultez [ec2-bundle-vol](#).

```
<block_device_mapping>  
  <mapping>  
    <virtual>ami</virtual>  
    <device>sda</device>  
  </mapping>  
  <mapping>  
    <virtual>ephemeral0</virtual>  
    <device>sdb</device>  
  </mapping>
```

```

<mapping>
  <virtual>ephemeral1</virtual>
  <device>sdc</device>
</mapping>
<mapping>
  <virtual>root</virtual>
  <device>/dev/sda1</device>
</mapping>
</block_device_mapping>

```

- d. Enregistrez le fichier `image.manifest.xml` et quittez votre éditeur de texte.
4. Pour charger votre bundle sur Amazon S3, exécutez la commande [ec2-upload-bundle](#) comme suit.

```
[ec2-user ~]$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

Important

Pour inscrire votre AMI dans une région autre que US East (N. Virginia), vous devez spécifier à la fois la région cible avec l'option `--region` et un chemin de compartiment qui existe déjà dans la région cible ou un chemin de compartiment unique qui peut être créé dans la région cible.

5. (Facultatif) Une fois que le groupe est chargé sur Amazon S3, vous pouvez le supprimer du répertoire `/tmp` sur l'instance en utilisant la commande `rm` suivante :

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

Important

Si vous avez spécifié un chemin avec l'option `-d` `/path/to/bundle/storage` dans [Step 2](#), utilisez ce chemin à la place de `/tmp`.

6. Pour inscrire votre AMI, exécutez la commande [register-image](#) comme suit.

```
[ec2-user ~]$ aws ec2 register-image --image-location my-s3-bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --virtualization-type hvm
```

⚠ Important

Si vous avez précédemment spécifié une région pour la commande [ec2-upload-bundle](#), spécifiez de nouveau cette région pour cette commande.

Créer une AMI à partir d'une instance Ubuntu basée sur un stockage d'instance

Cette section décrit la création d'une AMI à partir d'une instance Ubuntu Linux avec un volume de stockage d'instance comme volume racine. Il est possible que les procédures suivantes ne fonctionnent pas pour les instances exécutant d'autres distributions Linux. Pour les procédures spécifiques à Amazon Linux, consultez [Créer une AMI à partir d'une instance Amazon Linux basée sur un stockage d'instance](#).

Pour se préparer à utiliser les outils AMI (instances HVM uniquement)

Les outils AMI ont besoin de GRUB Legacy pour démarrer correctement. Toutefois, Ubuntu est configuré pour utiliser GRUB 2. Vous devez vérifier si votre instance utilise GRUB Legacy. Si non, vous devez l'installer et le configurer.

Les instances HVM ont également besoin que des outils de partitionnement soient installés pour que les outils AMI fonctionnent bien.

1. GRUB Legacy (version 0.9x ou inférieure) doit être installé sur votre instance. Vérifiez si GRUB Legacy est présent et installez-le si nécessaire.
 - a. Vérifiez la version de votre installation de GRUB.

```
ubuntu:~$ grub-install --version  
grub-install (GRUB) 1.99-21ubuntu3.10
```

Dans cet exemple, la version de GRUB est supérieure à 0.9x. Donc, GRUB Legacy doit être installée. Passez à [Step 1.b](#). Si GRUB Legacy est déjà présent, vous pouvez passer à l'[Step 2](#).

- b. Installez le package `grub` à l'aide de la commande suivante.

```
ubuntu:~$ sudo apt-get install -y grub
```

2. Installez les packages suivants de gestion de partition en utilisant le gestionnaire de package pour votre distribution.

- `gdisk` (certaines distributions peuvent appeler ce package `gptfdisk` à la place)
- `kpartx`
- `parted`

Utilisez la commande suivante.

```
ubuntu:~$ sudo apt-get install -y gdisk kpartx parted
```

3. Vérifiez les paramètres du noyau pour votre instance.

```
ubuntu:~$ cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-3.2.0-54-virtual root=UUID=4f392932-ed93-4f8f-
aee7-72bc5bb6ca9d ro console=ttyS0 xen_emul_unplug=unnecessary
```

Notez les options suivant les paramètres du noyau et du périphérique racine : `ro`, `console=ttyS0` et `xen_emul_unplug=unnecessary`. Vos options peuvent différer.

4. Vérifiez les entrées du noyau dans `/boot/grub/menu.lst`.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=hvc0
kernel /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
kernel /boot/memtest86+.bin
```

Notez que le paramètre `console` pointe vers `hvc0` au lieu de `ttyS0` et qu'il manque le paramètre `xen_emul_unplug=unnecessary`. Encore une fois, vos options peuvent différer.

5. Modifiez le fichier `/boot/grub/menu.lst` avec votre éditeur de texte préféré (comme `vim` ou `nano`) pour changer la console et ajoutez les paramètres que vous avez identifiés précédemment aux entrées de démarrage.

```
title          Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual
root           (hd0)
kernel         /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs
               ro console=ttyS0 xen_emul_unplug=unnecessary
initrd         /boot/initrd.img-3.2.0-54-virtual
```

```

title          Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual (recovery mode)
root           (hd0)
kernel        /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro
single console=ttyS0 xen_emul_unplug=unnecessary
initrd        /boot/initrd.img-3.2.0-54-virtual

title          Ubuntu 12.04.3 LTS, memtest86+
root           (hd0)
kernel        /boot/memtest86+.bin

```

6. Vérifiez que les entrées de votre noyau contiennent maintenant les bons paramètres.

```

ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=ttyS0
xen_emul_unplug=unnecessary
kernel /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
console=ttyS0 xen_emul_unplug=unnecessary
kernel /boot/memtest86+.bin

```

7. [Pour les versions Ubuntu 14.04 et ultérieures uniquement] Depuis la version Ubuntu 14.04, les AMI Ubuntu basées sur un stockage d'instance utilisent une table de partition GPT et une partition EFI séparée montée à l'emplacement `/boot/efi`. La commande `ec2-bundle-vol` ne regroupe pas cette partition de démarrage. Vous devez donc mettre en commentaire l'entrée `/etc/fstab` pour la partition EFI comme indiqué dans l'exemple suivant.

```

LABEL=cloudimg-rootfs /          ext4  defaults        0 0
#LABEL=UEFI           /boot/efi      vfat  defaults        0 0
/dev/xvdb             /mnt           auto  defaults,nobootwait,comment=cloudconfig 0 2

```

Pour créer une AMI à partir d'une instance Ubuntu basée sur un stockage d'instance

Cette procédure part du principe que vous avez respecté les prérequis dans [Prérequis](#).

Dans les commandes suivantes, remplacez chaque *espace réservé pour l'entrée utilisateur* par vos propres informations.

1. Chargez vos informations d'identification sur votre instance. Nous utilisons ces informations d'identification pour garantir que seuls vous et Amazon EC2 peuvent accéder à votre AMI.
 - a. Créez un répertoire temporaire sur votre instance pour vos informations d'identification en suivant ce qui suit :

```
ubuntu:~$ mkdir /tmp/cert
```

Ceci vous permet d'exclure vos informations d'identification de l'image créée.

- b. Copiez votre certificat X.509 et votre clé privée depuis votre ordinateur vers le répertoire /tmp/cert sur votre instance en utilisant un outil de copie sécurisé comme [scp](#). L'option -i *my-private-key.pem* de la commande scp suivante est la clé privée que vous utilisez pour vous connecter à votre instance avec SSH, et non la clé privée X.509. Exemples :

```
you@your_computer:~ $ scp -i my-private-key.pem /  
path/to/pk-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem /  
path/to/cert-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem ec2-  
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/  
pk-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem 100% 717 0.7KB/s 00:00  
cert-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem 100% 685 0.7KB/s 00:00
```

Sinon, étant donné qu'il s'agit de fichiers de texte brut, vous pouvez ouvrir le certificat et la clé dans un éditeur de texte et copier leur contenu dans de nouveaux fichiers dans le répertoire /tmp/cert.

2. Préparez le chargement du bundle sur Amazon S3 en exécutant la commande [ec2-bundle-vol](#) depuis votre instance. Assurez-vous de spécifier l'option -e pour exclure le répertoire où vos informations d'identification sont stockées. Par défaut, la création d'un bundle exclut les fichiers qui peuvent contenir des informations sensibles. Ces fichiers incluent *.sw, *.swo, *.swp, *.pem, *.priv, *id_rsa*, *id_dsa* *.gpg, *.jks, */.ssh/authorized_keys et */.bash_history. Pour inclure tous ces fichiers, utilisez l'option --no-filter. Pour inclure certains de ces fichiers, utilisez l'option --include.

Important

Par défaut, le processus de création d'un bundle d'AMI génère un ensemble de fichiers compressés et chiffrés dans le répertoire /tmp qui représente le volume racine. Si vous n'avez pas suffisamment d'espace disque libre dans /tmp pour stocker le groupe, vous devez spécifier un emplacement différent pour qu'il soit stocké avec l'option -d */path/to/bundle/storage*. Certaines instances disposent d'un stockage éphémère installé /mnt ou /media/ephemeral0 que vous pouvez utiliser, ou vous pouvez également créer, joindre et monter un nouveau volume Amazon (EBS) pour stocker le bundle. Pour

plus d'informations, consultez la section [Créer un volume Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

- a. Vous devez exécuter la commande `ec2-bundle-vol` en tant que racine. Pour la plupart des commandes, vous pouvez utiliser `sudo` afin d'obtenir des autorisations d'un niveau élevé, mais dans ce cas, vous devriez exécuter `sudo -E su` pour conserver vos variables d'environnement.

```
ubuntu:~$ sudo -E su
```

Notez que l'invite de commande de Bash vous identifie maintenant en tant qu'utilisateur racine, et que le signe dollar a été remplacé par un hashtag, ce qui indique que vous êtes dans un shell racine :

```
root@ubuntu:~#
```

- b. Pour créer le bundle AMI, exécutez la commande [ec2-bundle-vol](#) comme suit.

```
root@ubuntu:~# ec2-bundle-vol -k /tmp/cert/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u your_aws_account_id -r x86_64 -e /tmp/cert --partition gpt
```

Important

Pour les instances HVM de versions Ubuntu 14.04 et ultérieures, ajoutez l'indicateur `--partition mbr` pour regrouper correctement les instructions de démarrage. Sinon, votre AMI nouvellement créée ne démarrera pas.

La création de l'image peut prendre quelques minutes. Lorsque cette commande se termine, le répertoire `tmp` contient le groupe (`image.manifest.xml`), ainsi que plusieurs fichiers `image.part.xx`.

- c. Quittez le shell racine.

```
root@ubuntu:~# exit
```

3. (Facultatif) Pour ajouter davantage de volumes de stockage d'instance, modifiez les mappages de périphérique de stockage en mode bloc dans le fichier `image.manifest.xml` pour votre AMI. Pour plus d'informations, consultez [Mappages de périphériques de stockage en mode bloc](#).

- a. Créez une sauvegarde de votre fichier `image.manifest.xml`.

```
ubuntu:~$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

- b. Reformatez le fichier `image.manifest.xml` pour qu'il soit plus facile à lire et à modifier.

```
ubuntu:~$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/  
image.manifest.xml
```

- c. Modifiez les mappages de périphérique de stockage en mode bloc dans `image.manifest.xml` avec un éditeur de texte. L'exemple ci-dessous montre une nouvelle entrée pour le volume de stockage d'instance *ephemeral1*.

```
<block_device_mapping>  
  <mapping>  
    <virtual>ami</virtual>  
    <device>sda</device>  
  </mapping>  
  <mapping>  
    <virtual>ephemeral0</virtual>  
    <device>sdb</device>  
  </mapping>  
  <mapping>  
    <virtual>ephemeral1</virtual>  
    <device>sdc</device>  
  </mapping>  
  <mapping>  
    <virtual>root</virtual>  
    <device>/dev/sda1</device>  
  </mapping>  
</block_device_mapping>
```

- d. Enregistrez le fichier `image.manifest.xml` et quittez votre éditeur de texte.

4. Pour charger votre bundle sur Amazon S3, exécutez la commande [ec2-upload-bundle](#) comme suit.

```
ubuntu:~$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/  
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

⚠ Important

Si vous tentez d'inscrire votre AMI dans une région autre que US East (N. Virginia), vous devez spécifier à la fois la région cible avec l'option `--region` et un chemin de compartiment qui existe déjà dans la région cible ou un chemin de compartiment unique qui peut être créé dans la région cible.

5. (Facultatif) Une fois que le groupe est chargé sur Amazon S3, vous pouvez le supprimer du répertoire `/tmp` sur l'instance en utilisant la commande `rm` suivante :

```
ubuntu:~$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

⚠ Important

Si vous avez spécifié un chemin avec l'option `-d /path/to/bundle/storage` dans [Step 2](#), utilisez ce même chemin ci-dessous à la place de `/tmp`.

6. Pour inscrire votre AMI, exécutez la commande [register-image](#) AWS CLI comme suit.

```
ubuntu:~$ aws ec2 register-image --image-location my-s3-  
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --  
virtualization-type hvm
```

⚠ Important

Si vous avez précédemment spécifié une région pour la commande [ec2-upload-bundle](#), spécifiez de nouveau cette région pour cette commande.

7. [Pour les versions Ubuntu 14.04 et supérieures] Supprimez la mise en commentaire de l'entrée EFI dans `/etc/fstab`. Sinon, votre instance en cours d'exécution ne pourra pas redémarrer.

Convertir une AMI basée sur un stockage d'instance en AMI basée sur des volumes Amazon EBS

Vous pouvez convertir une AMI Linux basée sur un stockage d'instance que vous possédez en AMI basée sur des volumes Amazon EBS.

Important

Vous ne pouvez pas convertir une AMI qui ne vous appartient pas.

Pour convertir une AMI basée sur le stockage d'instance en une AMI basée sur des volumes Amazon EBS

1. Lancez une instance Amazon Linux à partir d'une AMI basée sur des volumes Amazon EBS. Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#). Les outils AWS CLI et AMI sont préinstallés sur les instances Amazon Linux.
2. Chargez la clé privée X.509 que vous avez utilisée pour grouper votre AMI basée sur le stockage d'instance vers votre instance. Nous utilisons cette clé pour garantir que seuls vous et Amazon EC2 peuvent accéder à votre AMI.
 - a. Créez un répertoire temporaire sur votre instance pour votre clé privée X.509 en suivant ce qui suit :

```
[ec2-user ~]$ mkdir /tmp/cert
```

- b. Copiez votre clé privée X.509 depuis votre ordinateur vers le répertoire /tmp/cert de votre instance en utilisant un outil de copie sécurisé comme [scp](#). Le paramètre *my-private-key* de la commande suivante est la clé privée que vous utilisez pour vous connecter à votre instance avec SSH. Par exemple :

```
you@your_computer:~ $ scp -i my-private-key.pem /  
path/to/pk-HKZYKTAIG2ECMXIYBH3HXV4ZBEXAMPLE.pem ec2-  
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/  
pk-HKZYKTAIG2ECMXIYBH3HXV4ZBEXAMPLE.pem 100% 717 0.7KB/s 00:00
```

3. Configurez vos variables d'environnement pour utiliser l' AWS CLI. Pour plus d'informations, consultez [Création d'une paire de clés](#).

- a. (Recommandé) Définissez des variables d'environnement pour votre clé AWS d'accès, votre clé secrète et votre jeton de session.

```
[ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
[ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
[ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
```

- b. Définissez des variables d'environnement pour votre clé AWS d'accès et votre clé secrète.

```
[ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
[ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
```

4. Préparer un volume Amazon Elastic Block Store (Amazon EBS) pour votre nouvelle AMI.

- a. Créez un volume EBS vide dans la même zone de disponibilité que votre instance à l'aide de la commande [create-volume](#). Notez l'ID du volume dans la sortie de la commande.

⚠ Important

Ce volume EBS doit avoir la même taille ou une taille plus importante que le volume racine de stockage d'instance original.

```
[ec2-user ~]$ aws ec2 create-volume --size 10 --region us-west-2 --
availability-zone us-west-2b
```

- b. Attachez le volume à votre instance basée sur Amazon EBS en utilisant la commande [attach-volume](#).

```
[ec2-user ~]$ aws ec2 attach-volume --volume-id volume_id --instance-
id instance_id --device /dev/sdb --region us-west-2
```

5. Créez un dossier pour votre groupe.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Téléchargez le groupe pour votre AMI basée sur le stockage d'instance sur /tmp/bundle en utilisant la commande [ec2-download-bundle](#).

```
[ec2-user ~]$ ec2-download-bundle -b my-s3-bucket/bundle_folder/bundle_name -m
image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --privatekey /
path/to/pk-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Reconstituez le fichier image à partir du groupe en utilisant la commande [ec2-unbundle](#).
 - a. Déplacez les répertoires vers le dossier du groupe.

```
[ec2-user ~]$ cd /tmp/bundle/
```

- b. Exécutez la commande [ec2-unbundle](#).

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem
```

8. Copiez les fichiers depuis l'image dégroupée vers le nouveau volume EBS.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Examinez le volume pour voir si de nouvelles partitions ont été dégroupées.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Affichez les périphériques de stockage en mode bloc pour trouver le nom du périphérique à monter.

```
[ec2-user bundle]$ lsblk
NAME          MAJ:MIN RM  SIZE RO  TYPE MOUNTPOINT
/dev/sda      202:0    0   8G  0  disk
##/dev/sda1   202:1    0   8G  0  part /
/dev/sdb      202:80   0  10G  0  disk
##/dev/sdb1   202:81   0  10G  0  part
```

Dans cet exemple, la partition à monter est `/dev/sdb1`, mais le nom de votre périphérique sera probablement différent. Si votre volume n'est pas partitionné, l'appareil à monter sera similaire à `/dev/sdb` (sans chiffre de fin de partition de périphérique).

11. Créez un point de montage pour le nouveau volume EBS et montez le volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
```

```
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Ouvrez le fichier `/etc/fstab` sur le volume EBS avec votre éditeur de texte préféré (comme `vim` ou `nano`) et supprimez toutes les entrées pour les volumes (éphémères) de stockage d'instance. Étant donné que le volume EBS est monté sur `/mnt/ebs`, le fichier `fstab` se situe à l'emplacement `/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/      /          ext4      defaults,noatime 1 1
tmpfs       /dev/shm  tmpfs    defaults      0 0
devpts      /dev/pts  devpts   gid=5,mode=620 0 0
sysfs       /sys      sysfs    defaults      0 0
proc        /proc     proc     defaults      0 0
/dev/sdb    /media/ephemeral0 auto     defaults,comment=cloudconfig 0
2
```

Dans cet exemple, la dernière ligne devrait être supprimée.

13. Démontez le volume et détachez-le de l'instance.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id volume_id --region us-west-2
```

14. Créez une AMI à partir du nouveau volume EBS comme suit.

- a. Créez un instantané du nouveau volume EBS.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description "your_snapshot_description" --volume-id volume_id
```

- b. Vérifiez si votre instantané est terminé.

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-id snapshot_id
```

- c. Identifiez l'architecture de processeur, le type de virtualisation et l'image noyau (aki) utilisée sur l'AMI originale avec la commande `describe-images`. Pour cette étape, vous avez besoin de l'ID d'AMI de l'AMI d'origine basée sur un stockage d'instance.

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-id ami-id --output text
```

```
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
available public machine aki-fc8f11cc instance-store paravirtual xen
```

Dans cet exemple, l'architecture est `x86_64` et l'ID de l'image noyau est `aki-fc8f11cc`. Utilisez ces valeurs dans l'étape suivante. Si le résultat de la commande ci-dessus liste aussi un ID `ari`, prenez également note de cela.

- d. Enregistrez votre nouvelle AMI avec l'ID d'instantané de votre nouveau volume EBS et les valeurs de l'étape précédente. Si la sortie de la commande précédente a répertorié un ID `ari`, incluez-le dans la commande suivante avec `--ramdisk-id ari_id`.

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
name your_new_ami_name --block-device-mappings DeviceName=device-
name,Ebs={SnapshotId=snapshot_id} --virtualization-type paravirtual --
architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Facultatif) Après avoir vérifié que vous pouvez lancer une instance à partir de votre nouvelle AMI, vous pouvez supprimer le volume EBS que vous avez créé pour cette procédure.

```
aws ec2 delete-volume --volume-id volume_id
```

Référence des outils AMI

Vous pouvez utiliser les commandes des outils AMI pour créer et gérer des AMI Linux basées sur le stockage d'instance. Pour installer les outils, consultez [Configurer les outils AMI](#).

Pour plus d'informations sur vos clés d'accès, consultez [Bonnes pratiques pour les comptes AWS](#) dans le Guide de référence AWS Account Management .

Commandes

- [ec2-ami-tools-version](#)
- [ec2-bundle-image](#)
- [ec2-bundle-vol](#)
- [ec2-delete-bundle](#)
- [ec2-download-bundle](#)
- [ec2-migrate-manifest](#)
- [ec2-unbundle](#)

- [ec2-upload-bundle](#)
- [Options courantes pour les outils AMI](#)

ec2-ami-tools-version

Description

Décrit la version des outils AMI.

Syntaxe

ec2-ami-tools-version

Sortie

Informations de version.

Exemple

Cet exemple de commande affiche les informations de version des outils AMI que vous utilisez.

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

ec2-bundle-image

Description

Crée une AMI Linux basée sur le stockage d'instance à partir d'une image du système d'exploitation créée dans un fichier de boucle.

Syntaxe

```
ec2-bundle-image -c path -k path -u account -i path [-d path] [--ec2cert path] [-r architecture] [--productcodes code1,code2,...] [-B mapping] [-p prefix]
```

Options

-c, --cert chemin

Fichier de certificat de clé publique RSA code PEM de l'utilisateur.

Obligatoire : oui

`-k, --privatekey chemin`

Chemin d'accès à un fichier de clé RSA codée PEM. Vous devrez également spécifier cette clé pour dissocier ce groupe, conservez-la dans un endroit sûr. Notez qu'il n'est pas nécessaire que la clé soit enregistrée sur votre AWS compte.

Obligatoire : oui

`-u, --user compte`

L'identifiant du AWS compte de l'utilisateur, sans tirets.

Obligatoire : oui

`-i, --image chemin`

Chemin d'accès à l'image à grouper.

Obligatoire : oui

`-d, --destination chemin`

Répertoire dans lequel vous créez le groupe.

Par défaut: `/tmp`

Obligatoire : non

`--ec2cert chemin`

Chemin d'accès au certificat de clé publique Amazon EC2 X.509 utilisé pour chiffrer le manifeste de l'image.

Les régions `us-gov-west-1` et `cn-north-1` utilisent un certificat de clé publique par défaut. Le chemin d'accès à ce certificat doit être spécifié avec cette option. Le chemin d'accès au certificat varie selon la méthode d'installation des outils AMI. Pour Amazon Linux, les certificats se trouvent à l'adresse `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Si vous avez installé les outils AMI à partir du fichier RPM ou ZIP dans [Configurer les outils AMI](#), les certificats se trouvent à l'adresse `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obligatoire : uniquement pour les régions `us-gov-west-1` et `cn-north-1`.

`-r, --arch architecture`

Architecture d'image. Si vous ne fournissez pas l'architecture dans la ligne de commande, vous serez invité à la saisir au début de la création du bundle.

Valeurs valides : `i386` | `x86_64`

Obligatoire : non

`--productcodes` `code1,code2,...`

Codes de produit à attacher à l'image au moment de l'inscription, séparé par des virgules.

Obligatoire : non

`-B, --block-device-mapping` `mappage`

Définit la façon dont les périphériques de stockage en mode bloc sont exposés à une instance de AMI si son type d'instance prend en charge le périphérique spécifié.

Spécifiez une liste séparée par des virgules de paires clé-valeur, où chaque clé est un nom virtuel et chaque valeur le nom de périphérique correspondant. Les noms virtuels incluent les éléments suivants :

- `ami`— Périphérique du système de fichiers racine, tel qu'il est vu par l'instance
- `root`— Périphérique du système de fichiers racine, tel qu'il est vu par le noyau
- `swap`— Périphérique d'échange, tel qu'il est vu par l'instance
- `ephemeralN`—Volume de stockage de la nième instance

Obligatoire : non

`-p, --prefix` `prefix`

Préfixe du nom des fichiers AMI groupés.

Par défaut : nom du fichier image. Par exemple, si le chemin d'accès de l'image est `/var/spool/my-image/version-2/debian.img`, le préfixe par défaut est `debian.img`.

Obligatoire : non

`--kernel` `kernel_id`

Obsolète. Utilisez [register-image](#) pour définir le noyau.

Obligatoire : non

`--ramdisk` `ramdisk_id`

Obsolète. Utilisez [register-image](#) pour définir le disque RAM le cas échéant.

Obligatoire : non

Sortie

Messages d'état décrivant les étapes et le statut du processus de groupement.

Exemple

Cet exemple crée une AMI groupée à partir d'une image du système d'exploitation qui a été créée dans un fichier de boucle.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

Description

Crée une AMI Linux basée sur le stockage d'instance par compression, chiffrement et signature d'une copie du volume du périphérique racine de l'instance.

Amazon EC2 tente d'hériter les codes de produit, les paramètres du noyau, les paramètres du disque RAM et les mappages du périphérique de stockage en mode bloc de l'instance.

Par défaut, la création d'un bundle exclut les fichiers qui peuvent contenir des informations sensibles. Ces fichiers incluent *.sw, *.swo, *.swp, *.pem, *.priv, *id_rsa*, *id_dsa* *.gpg, *.jks, */.ssh/authorized_keys et */.bash_history. Pour inclure tous ces fichiers, utilisez l'option --no-filter. Pour inclure certains de ces fichiers, utilisez l'option --include.

Pour plus d'informations, consultez [Créer une AMI Linux basée sur le stockage d'instance](#).

Syntaxe

```
ec2-bundle-vol -c path -k path -u account [-d path] [--ec2cert path] [-r architecture] [--productcodes code1,code2,...] [-B mapping] [--all] [-e directory1,directory2,...] [-i file1,file2,...] [--no-filter] [-p prefix] [-s size] [--[no-]inherit] [-v volume] [-P type] [-S script] [--fstab path] [--generate-fstab] [--grub-config path]
```

Options

-c, --cert chemin

Fichier de certificat de clé publique RSA code PEM de l'utilisateur.

Obligatoire : oui

-k, --privatekey chemin

Chemin d'accès au fichier de clé RSA codé PEM de l'utilisateur.

Obligatoire : oui

-u, --user compte

L'identifiant du AWS compte de l'utilisateur, sans tirets.

Obligatoire : oui

-d, --destination destination

Répertoire dans lequel vous créez le groupe.

Par défaut: /tmp

Obligatoire : non

`--ec2cert` chemin

Chemin d'accès au certificat de clé publique Amazon EC2 X.509 utilisé pour chiffrer le manifeste de l'image.

Les régions `us-gov-west-1` et `cn-north-1` utilisent un certificat de clé publique par défaut. Le chemin d'accès à ce certificat doit être spécifié avec cette option. Le chemin d'accès au certificat varie selon la méthode d'installation des outils AMI. Pour Amazon Linux, les certificats se trouvent à l'adresse `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Si vous avez installé les outils AMI à partir du fichier RPM ou ZIP dans [Configurer les outils AMI](#), les certificats se trouvent à l'adresse `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obligatoire : uniquement pour les régions `us-gov-west-1` et `cn-north-1`.

`-r, --arch` architecture

Architecture de l'image. Si vous ne fournissez pas cette ligne de commande, vous serez invité à la saisir au début de la création du bundle.

Valeurs valides : `i386` | `x86_64`

Obligatoire : non

`--productcodes` code1,code2,...

Codes de produit à attacher à l'image au moment de l'inscription, séparé par des virgules.

Obligatoire : non

`-B, --block-device-mapping` mappage

Définit la façon dont les périphériques de stockage en mode bloc sont exposés à une instance de AMI si son type d'instance prend en charge le périphérique spécifié.

Spécifiez une liste séparée par des virgules de paires clé-valeur, où chaque clé est un nom virtuel et chaque valeur le nom de périphérique correspondant. Les noms virtuels incluent les éléments suivants :

- `ami`— Périphérique du système de fichiers racine, tel qu'il est vu par l'instance
- `root`— Périphérique du système de fichiers racine, tel qu'il est vu par le noyau
- `swap`— Périphérique d'échange, tel qu'il est vu par l'instance

- ephemeralN—Volume de stockage de la nième instance

Obligatoire : non

-a, --all

Groupez tous les répertoires, y compris ceux contenus dans les systèmes de fichiers montés à distance.

Obligatoire : non

-e, --exclude directory1,directory2,...

Liste des chemins absolus de répertoires et fichiers à exclure de l'opération de groupement. Ce paramètre remplace l'option --all. Lorsque la commande exclude est spécifié, les répertoires et sous-répertoires répertoriés avec le paramètre ne sont pas groupés avec le volume.

Obligatoire : non

-i, --include file1,file2,...

Liste des fichiers à inclure dans l'opération de groupement. Les fichiers spécifiés seraient autrement exclus de l'AMI car ils peuvent contenir des informations sensibles.

Obligatoire : non

--no-filter

Si ce paramètre est spécifié, nous n'excluons pas les fichiers de l'AMI, car ils peuvent contenir des informations sensibles.

Obligatoire : non

-p, --prefix prefix

Préfixe du nom des fichiers AMI groupés.

Par défaut: image

Obligatoire : non

-s, --size taille

Taille, en Mo (1024 * 1024 octets), du fichier image à créer. La taille maximale est 10 240 Mo.

Par défaut: 10240

Obligatoire : non

`--[no-]inherit`

Indique si l'image doit hériter des métadonnées de l'instance (la valeur par défaut consiste à hériter). Le groupement échoue si vous activez `--inherit`, mais les métadonnées d'instance ne sont pas accessibles.

Obligatoire : non

`-v, --volume volume`

Chemin d'accès absolu au volume monté à partir duquel créer le groupe.

Par défaut : le répertoire racine (/)

Obligatoire : non

`-P, --partition type`

Indique si l'image de disque doit utiliser une table de partition. Si vous ne spécifiez pas de type de table de partition, la valeur par défaut est le type utilisé sur le périphérique de stockage en mode bloc parent du volume, le cas échéant. Dans le cas contraire, la valeur par défaut est `gpt`.

Valeurs valides : `mbr | gpt | none`

Obligatoire : non

`-S, --script script`

Script de personnalisation à exécuter juste avant de procéder à la création du bundle. Le script doit attendre un seul argument, le point de montage du volume.

Obligatoire : non

`--fstab chemin`

Chemin d'accès au fichier `fstab` à grouper dans l'image. S'il n'est pas spécifié, Amazon EC2 groupe `/etc/fstab`.

Obligatoire : non

`--generate-fstab`

Groupe le volume grâce au fichier `fastab` fourni par Amazon EC2.

Obligatoire : non

`--grub-config`

Chemin d'accès à un autre fichier de configuration grub à grouper dans l'image. Par défaut, `ec2-bundle-vol` attend `/boot/grub/menu.lst` ou `/boot/grub/grub.conf` pour exister sur l'image clonée. Cette option vous permet de spécifier un chemin d'accès à un autre fichier de configuration grub, qui sera ensuite copié par-dessus les valeurs par défaut (le cas échéant).

Obligatoire : non

`--kernel kernel_id`

Obsolète. Utilisez [register-image](#) pour définir le noyau.

Obligatoire : non

`--ramdiskramdisk_id`

Obsolète. Utilisez [register-image](#) pour définir le disque RAM le cas échéant.

Obligatoire : non

Sortie

Messages d'état décrivant les étapes et le statut de la création du bundle.

Exemple

Cet exemple crée un groupe AMI par compression, chiffrement et signature d'un instantané du système de fichiers racine de l'ordinateur local.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem -c
cert-HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
Copying / into the image file /mnt/image...
Excluding:
  sys
  dev/shm
  proc
  dev/pts
  proc/sys/fs/binfmt_misc
  dev
  media
```

```
mnt
proc
sys
tmp/image
mnt/img-mnt
1+0 records in
1+0 records out
mke2fs 1.38 (30-Jun-2005)
warning: 256 blocks unused.

Splitting /mnt/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
...
Created image.part.22
Created image.part.23
Generating digests for each part...
Digests generated.
Creating bundle manifest...
Bundle Volume complete.
```

ec2-delete-bundle

Description

Supprime le groupe spécifié du stockage Amazon S3. Une fois que vous supprimez un groupe, vous ne pouvez pas lancer d'instances à partir de l'AMI correspondante.

Syntaxe

```
ec2-delete-bundle -b bucket -a access_key_id -s secret_access_key [-t token] [--url url] [--region region] [--sigv version] [-m path] [-p prefix] [--clear] [--retry] [-y]
```

Options

-b, --bucket *bucket*

Le nom du compartiment Amazon S3 contenant l'AMI groupée, suivi d'un préfixe de chemin facultatif séparé par des « / »

Obligatoire : oui

-a, --access-key access_key_id

L'ID de la clé d' AWS accès.

Obligatoire : oui

-s, --secret-key secret_access_key

La clé d'accès AWS secrète.

Obligatoire : oui

-t, --delegation-token jeton

Le jeton de délégation à transmettre à la AWS demande. Pour plus d'informations, consultez [Utilisation des autorisations de sécurité temporaires](#).

Requis : uniquement lorsque vous utilisez des informations d'identification de sécurité temporaires.

Par défaut : valeur de la variable d'environnement AWS_DELEGATION_TOKEN (si elle est définie).

--regionregion

Région à utiliser dans la signature de la demande.

Par défaut : us-east-1

Requis : requis si vous utilisez Signature Version 4

--sigvVersion

Version de signature à utiliser lors de la signature de la demande.

Valeurs valides : 2 | 4

Par défaut: 4

Obligatoire : non

-m, --manifestchemin

Chemin d'accès au fichier manifeste.

Requis : vous devez spécifier `--prefix` ou `--manifest`.

`-p, --prefix prefix`

Préfixe du nom de fichier AMI groupé. Fournissez le préfixe entier. Par exemple, si le préfixe est `image.img`, utilisez `-p image.img`, non `-p image`.

Requis : vous devez spécifier `--prefix` ou `--manifest`.

`--clear`

Supprime le compartiment Amazon S3 s'il est vide après la suppression du groupe spécifié.

Obligatoire : non

`--retry`

Refait automatiquement des tentatives sur toutes les erreurs Amazon S3, jusqu'à cinq fois par opération.

Obligatoire : non

`-y, --yes`

Suppose automatiquement que la réponse à toutes les invites est oui.

Obligatoire : non

Sortie

Amazon EC2 affiche les messages d'état indiquant les étapes et le statut du processus de suppression.

Exemple

Cet exemple supprime un groupe de Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b DOC-EXAMPLE-BUCKET1 -a your_access_key_id -s your_secret_access_key
Deleting files:
DOC-EXAMPLE-BUCKET1/image.manifest.xml
DOC-EXAMPLE-BUCKET1/image.part.00
DOC-EXAMPLE-BUCKET1/image.part.01
```

```
DOC-EXAMPLE-BUCKET1/image.part.02
DOC-EXAMPLE-BUCKET1/image.part.03
DOC-EXAMPLE-BUCKET1/image.part.04
DOC-EXAMPLE-BUCKET1/image.part.05
DOC-EXAMPLE-BUCKET1/image.part.06
Continue? [y/n]
y
Deleted DOC-EXAMPLE-BUCKET1/image.manifest.xml
Deleted DOC-EXAMPLE-BUCKET1/image.part.00
Deleted DOC-EXAMPLE-BUCKET1/image.part.01
Deleted DOC-EXAMPLE-BUCKET1/image.part.02
Deleted DOC-EXAMPLE-BUCKET1/image.part.03
Deleted DOC-EXAMPLE-BUCKET1/image.part.04
Deleted DOC-EXAMPLE-BUCKET1/image.part.05
Deleted DOC-EXAMPLE-BUCKET1/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Description

Télécharge les AMIs Linux basées sur le stockage d'instance depuis le stockage Amazon S3.

Syntaxe

```
ec2-download-bundle -b bucket -a access_key_id -s secret_access_key -k path  
[--url url] [--region region] [--sigv version] [-m file] [-p prefix] [-d  
directory] [--retry]
```

Options

-b, --bucket *bucket*

Nom du compartiment Amazon S3 où se trouve le groupe, suivi d'un préfixe de chemin séparé par des « / »-facultatif.

Obligatoire : oui

-a, --access-key *access_key_id*

L'ID de la clé d' AWS accès.

Obligatoire : oui

`-s, --secret-key secret_access_key`

La clé d'accès AWS secrète.

Obligatoire : oui

`-k, --privatekey chemin`

Clé privée utilisée pour déchiffrer le manifeste.

Obligatoire : oui

`--url url`

URL du service Amazon S3.

Par défaut: `https://s3.amazonaws.com/`

Obligatoire : non

`--region région`

Région à utiliser dans la signature de la demande.

Par défaut : `us-east-1`

Requis : requis si vous utilisez Signature Version 4

`--sigv version`

Version de signature à utiliser lors de la signature de la demande.

Valeurs valides : 2 | 4

Par défaut: 4

Obligatoire : non

`-m, --manifest file`

Nom du fichier manifeste (sans le chemin d'accès). Nous vous recommandons de spécifier soit le manifeste (`-m`) soit un préfixe (`-p`).

Obligatoire : non

`-p, --prefix prefix`

Préfixe du nom des fichiers AMI groupés.

Par défaut: image

Obligatoire : non

-d, --directory directory

Répertoire dans lequel le groupe téléchargé est enregistré. Le répertoire doit exister.

Par défaut : le répertoire de travail actuel.

Obligatoire : non

--retry

Refait automatiquement des tentatives sur toutes les erreurs Amazon S3, jusqu'à cinq fois par opération.

Obligatoire : non

Sortie

Les messages d'état indiquant les différentes étapes du processus de téléchargement s'affichent.

Exemple

Cet exemple crée le répertoire `bundled` (à l'aide de la commande Linux `mkdir`) et télécharge le groupe depuis le compartiment Amazon S3 `DOC-EXAMPLE-BUCKET1`.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name
-m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from DOC-EXAMPLE-BUCKET1 to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
mybundle/image.part.00 ...
Downloaded image.part.00 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.01 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
mybundle/image.part.01 ...
Downloaded image.part.01 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.02 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
mybundle/image.part.02 ...
Downloaded image.part.02 from DOC-EXAMPLE-BUCKET1
```

```
Downloading part image.part.03 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
mybundle/image.part.03 ...
Downloaded image.part.03 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.04 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
mybundle/image.part.04 ...
Downloaded image.part.04 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.05 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
mybundle/image.part.05 ...
Downloaded image.part.05 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.06 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
mybundle/image.part.06 ...
Downloaded image.part.06 from DOC-EXAMPLE-BUCKET1
```

ec2-migrate-manifest

Description

Modifie une AMI Linux basée sur le stockage d'instance (par exemple, son certificat, son noyau et son disque RAM) de sorte qu'elle prenne en charge une autre région.

Syntaxe

```
ec2-migrate-manifest -c path -k path -m path {(-a access_key_id -s secret_access_key --region region) | (--no-mapping)} [--ec2cert ec2_cert_path] [--kernel kernel-id] [--ramdisk ramdisk_id]
```

Options

-c, --cert chemin

Fichier de certificat de clé publique RSA code PEM de l'utilisateur.

Obligatoire : oui

-k, --privatekey chemin

Chemin d'accès au fichier de clé RSA codé PEM de l'utilisateur.

Obligatoire : oui

--manifest chemin

Chemin d'accès au fichier manifeste.

Obligatoire : oui

-a, --access-key access_key_id

L'ID de la clé d' AWS accès.

Requis : requis si vous utilisez le mappage automatique.

-s, --secret-key secret_access_key

La clé d'accès AWS secrète.

Requis : requis si vous utilisez le mappage automatique.

--region région

Région à rechercher dans le fichier de mappage.

Requis : requis si vous utilisez le mappage automatique.

--no-mapping

Désactive le mappage automatique des noyaux et disques RAM.

Lors de la migration, Amazon EC2 remplace le noyau et le disque RAM dans le fichier manifeste par un noyau et un disque RAM conçus pour la région de destination. Si le paramètre --no-mapping n'est pas fourni, `ec2-migrate-bundle` peut utiliser les opérations `DescribeRegions` et `DescribeImages` pour effectuer les mappages automatiques.

Requis : requis si vous ne fournissez pas les options -a, -s et --region utilisées pour le mappage automatique.

--ec2cert chemin

Chemin d'accès au certificat de clé publique Amazon EC2 X.509 utilisé pour chiffrer le manifeste de l'image.

Les régions `us-gov-west-1` et `cn-north-1` utilisent un certificat de clé publique par défaut. Le chemin d'accès à ce certificat doit être spécifié avec cette option. Le chemin d'accès au certificat varie selon la méthode d'installation des outils AMI. Pour Amazon Linux, les certificats se trouvent à l'adresse `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Si vous avez installé les outils AMI à partir du fichier ZIP dans [Configurer les outils AMI](#), les certificats se trouvent à l'adresse `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obligatoire : uniquement pour les régions `us-gov-west-1` et `cn-north-1`.

`--kernel kernel_id`

ID du noyau à sélectionner.

 Important

Nous vous recommandons d'utiliser PV-GRUB au lieu des noyaux et des disques RAM. Pour plus d'informations, consultez la section [Noyaux fournis par l'utilisateur](#) dans le guide de l'utilisateur Amazon Linux 2.

Obligatoire : non

`--ramdisk ramdisk_id`

ID du disque RAM à sélectionner.

 Important

Nous vous recommandons d'utiliser PV-GRUB au lieu des noyaux et des disques RAM. Pour plus d'informations, consultez la section [Noyaux fournis par l'utilisateur](#) dans le guide de l'utilisateur Amazon Linux 2.

Obligatoire : non

Sortie

Messages d'état décrivant les étapes et le statut du processus de groupement.

Exemple

Cet exemple copie l'AMI spécifiée dans le fichier manifeste `my-ami.manifest.xml` depuis les États-Unis vers l'Union européenne.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml
--cert cert-HKZYKTAIG2ECMXIYIBH3HXV4ZBZQ55CL0.pem --privatekey pk-
HKZYKTAIG2ECMXIYIBH3HXV4ZBZQ55CL0.pem --region eu-west-1
```

```
Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

Description

Recrée le groupe à partir d'une AMI Linux basée sur le stockage d'instance.

Syntaxe

```
ec2-unbundle -k path -m path [-s source_directory] [-d destination_directory]
```

Options

-k, --privatekey chemin

Chemin d'accès à votre fichier de clé RSA codée PEM.

Obligatoire : oui

-m, --manifest chemin

Chemin d'accès au fichier manifeste.

Obligatoire : oui

-s, --source *source_directory*

Répertoire contenant le groupe.

Par défaut : le répertoire actuel.

Obligatoire : non

-d, --destination *destination_directory*

Répertoire dans lequel dégroupier l'AMI. Le répertoire de destination doit exister.

Par défaut : le répertoire actuel.

Obligatoire : non

Exemple

Cet exemple Linux et UNIX dégroupé l'AMI spécifiée dans le fichier `image.manifest.xml`.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-
HKZYKTAIG2ECMXIYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

Sortie

Les messages d'état indiquant les différentes étapes du processus de dégroupement s'affichent.

ec2-upload-bundle

Description

Charge la solution groupée d'une AMI Linux basée sur le stockage d'instances vers Amazon S3 et définit les listes de contrôle d'accès (ACL) appropriées au niveau des objets chargés. Pour plus d'informations, consultez [Créer une AMI Linux basée sur le stockage d'instance](#).

Note

Afin de charger des objets vers un compartiment S3 pour votre AMI Linux basée sur le stockage d'instances, les listes de contrôle d'accès doivent être activées pour le compartiment. Sinon, Amazon EC2 ne sera pas en mesure de définir des listes ACL sur les objets à charger. Si votre compartiment de destination utilise le paramètre appliqué par le propriétaire du compartiment pour la propriété de l'objet S3 (S3 Object Ownership), cela ne fonctionnera pas car les listes de contrôle d'accès sont désactivées. Pour plus d'informations, consultez la section [Contrôle de la propriété des objets chargés à l'aide de la propriété de l'objet S3](#).

Syntaxe

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t token] -m path [--url url] [--region region] [--sigv version] [--acl acl] [-d directory] [--part part] [--retry] [--skipmanifest]
```

Options

`-b, --bucket bucket`

Nom du compartiment Amazon S3 dans lequel stocker le groupe, suivi d'un préfixe de chemin séparé par des « / » facultatif. Si le compartiment n'existe pas, il est créé si le nom de compartiment est disponible. De plus, si le compartiment n'existe pas et que la version des outils AMI est la version 1.5.18 ou toute autre version ultérieure, cette commande définit les ACL du compartiment.

Obligatoire : oui

`-a, --access-key access_key_id`

L'identifiant de votre clé d'AWS accès.

Obligatoire : oui

`-s, --secret-key secret_access_key`

Votre clé d'accès AWS secrète.

Obligatoire : oui

`-t, --delegation-token jeton`

Le jeton de délégation à transmettre à la AWS demande. Pour plus d'informations, consultez [Utilisation des autorisations de sécurité temporaires](#).

Requis : uniquement lorsque vous utilisez des informations d'identification de sécurité temporaires.

Par défaut : valeur de la variable d'environnement `AWS_DELEGATION_TOKEN` (si elle est définie).

`-m, --manifest chemin`

Chemin d'accès au fichier manifeste. Le fichier manifeste est créé pendant la création d'un bundle ; il est disponible dans le répertoire contenant le groupe.

Obligatoire : oui

`--url url`

Obsolète. Utilisez plutôt l'option `--region`, sauf si votre compartiment est limité à l'emplacement EU (et pas eu-west-1). L'indicateur `--location` est le seul moyen de cibler cette restriction d'emplacement spécifique.

URL du service de point de terminaison Amazon S3.

Par défaut: `https://s3.amazonaws.com/`

Obligatoire : non

`--region` région

Région à utiliser dans la signature de la demande pour le compartiment de destination S3.

- Si le compartiment n'existe pas et que vous ne spécifiez pas une région, l'outil crée le compartiment sans contrainte d'emplacement (dans `us-east-1`).
- Si le compartiment n'existe pas et que vous spécifiez une région, l'outil crée le compartiment dans la région spécifiée.
- Si le compartiment existe et que vous ne spécifiez pas une région, l'outil utilise emplacement du compartiment.
- Si le compartiment existe et que vous spécifiez `us-east-1` comme région, l'outil utilise l'emplacement du compartiment sans aucun message d'erreur, tous les fichiers correspondants existants sont écrasés.
- Si le compartiment existe et que vous spécifiez une région (autre que `us-east-1`) qui ne correspond pas à l'emplacement du compartiment, l'outil se termine avec une erreur.

Si votre compartiment est limité à l'emplacement EU (et pas `eu-west-1`), utilisez plutôt l'indicateur `--location`. L'indicateur `--location` est le seul moyen de cibler cette restriction d'emplacement spécifique.

Par défaut : `us-east-1`

Requis : requis si vous utilisez Signature Version 4

`--sigv` version

Version de signature à utiliser lors de la signature de la demande.

Valeurs valides : 2 | 4

Par défaut: 4

Obligatoire : non

`--acl` acl

Stratégie de liste de contrôle des accès de l'image groupée.

Valeurs valides : `public-read` | `aws-exec-read`

Par défaut: `aws-exec-read`

Obligatoire : non

`-d, --directory directory`

Répertoire contenant les parties de l'AMI groupée.

Par défaut : le répertoire contenant le fichier manifeste (cf. l'option `-m`).

Obligatoire : non

`--part part`

Commence le chargement de la partie spécifiée et de toutes les parties suivantes. Par exemple, `--part 04`.

Obligatoire : non

`--retry`

Refait automatiquement des tentatives sur toutes les erreurs Amazon S3, jusqu'à cinq fois par opération.

Obligatoire : non

`--skipmanifest`

Ne charge pas le fichier manifeste.

Obligatoire : non

`--location location`

Obsolète. Utilisez plutôt l'option `--region`, sauf si votre compartiment est limité à l'emplacement EU (et pas `eu-west-1`). L'indicateur `--location` est le seul moyen de cibler cette restriction d'emplacement spécifique.

Contrainte d'emplacement du compartiment Amazon S3 de destination. Si le compartiment existe et que vous spécifiez un emplacement qui ne correspond pas à l'emplacement du compartiment, l'outil se termine avec une erreur. Si le compartiment existe et que vous ne spécifiez pas d'emplacement, l'outil utilise l'emplacement du compartiment. Si le compartiment n'existe pas et que vous spécifiez un emplacement, l'outil crée le compartiment dans l'emplacement spécifié.

Si le compartiment n'existe pas et que vous ne spécifiez pas d'emplacement, l'outil crée le compartiment sans contrainte d'emplacement (dans `us-east-1`).

Par défaut : si `--region` est spécifié, l'emplacement est défini sur cette région spécifiée. Si `--region` n'est pas spécifié, l'emplacement par défaut est `us-east-1`.

Obligatoire : non

Sortie

Amazon EC2 affiche les messages d'état qui indiquent les étapes et l'état du processus de chargement.

Exemple

Cet exemple télécharge le groupe spécifié par le fichier manifeste `image.manifest.xml`.

```
[ec2-user ~]$ ec2-upload-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name -m
image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket DOC-EXAMPLE-BUCKET1 ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

Options courantes pour les outils AMI

La plupart des outils AMI acceptent les paramètres facultatifs suivants.

`--help, -h`

Affiche le message d'aide.

`--version`

Affiche la version et l'avis de droit d'auteur.

`--manual`

Affiche l'entrée manuelle.

`--batch`

S'exécute en mode de traitement par lots et supprime les invites interactives.

`--debug`

Affiche les informations qui peuvent être utiles pour la résolution de problèmes.

Création d'une AMI avec Windows Sysprep

L'outil System Preparation (Sysprep) simplifie le processus de duplication d'une installation personnalisée de Microsoft Windows. Vous pouvez utiliser Sysprep pour créer une image Amazon Machine Image (AMI) standardisée. Vous pouvez ensuite créer de nouvelles instances Amazon EC2 pour Windows en vous basant sur cette image standardisée.

Nous vous recommandons d'utiliser [EC2 Image Builder](#) pour automatiser la création, la gestion et le déploiement d'images de serveur personnalisées, sécurisées up-to-date et « dorées » préinstallées et préconfigurées avec des logiciels et des paramètres.

Si vous utilisez Windows Sysprep pour créer une AMI standardisée, nous vous recommandons d'exécuter Sysprep avec [EC2Launch v2](#). Si vous utilisez encore les agents EC2Config (Windows Server 2012 R2 et versions antérieures) ou EC2Launch (Windows Server 2016 et 2019), consultez la documentation relative à l'utilisation de Sysprep avec EC2Config et EC2Launch ci-dessous.

Important

N'utilisez pas Sysprep pour créer une sauvegarde d'instance. Sysprep supprime les informations spécifiques au système. Cela peut entraîner des conséquences imprévues pour une sauvegarde d'instance.

Pour résoudre les problèmes liés à Sysprep, consultez [Résoudre les problèmes liés à Sysprep avec les instances Windows](#).

Sommaire

- [Avant de commencer](#)
- [Utiliser Sysprep avec EC2Launch v2](#)
- [Utiliser Sysprep avec EC2Launch](#)
- [Utiliser Sysprep avec EC2Config](#)

Avant de commencer

- Avant d'exécuter Sysprep, nous vous recommandons de supprimer tous les comptes d'utilisateur locaux et tous les profils de compte autres que le compte d'administrateur individuel sous lequel Sysprep sera exécuté. Si vous exécutez Sysprep avec des comptes et des profils supplémentaires, un comportement inattendu peut en résulter, y compris la perte de données de profil ou l'échec d'exécution de Sysprep.
- En savoir plus sur [Sysprep sur Microsoft](#). TechNet
- Découvrez quels [rôles de serveur sont pris en charge pour Sysprep](#).

Utiliser Sysprep avec EC2Launch v2

Cette section contient des détails sur les différentes phases d'exécution de Sysprep et les tâches effectuées par le service EC2Launch v2 lors de la préparation de l'image. Il inclut également les étapes pour créer une AMI normalisée à l'aide de Sysprep avec le service EC2Launch v2.

Sysprep avec des rubriques EC2Launch v2

- [Phases Sysprep](#)
- [Actions Sysprep](#)
- [Étapes post-actions Sysprep](#)
- [Exécution de Sysprep avec EC2Launch v2](#)

Phases Sysprep

Sysprep passe par les phases suivantes :

- **Generalize** : l'outil supprime les informations et les configurations spécifiques à l'image. Par exemple, Sysprep supprime l'identificateur de sécurité (SID), le nom de l'ordinateur, les journaux d'événements et des pilotes spécifiques, pour n'en citer que quelques-uns. Une fois cette phase terminée, le système d'exploitation est prêt à créer une AMI.

Note

Lorsque vous exécutez Sysprep avec le service EC2Launch v2, le système empêche la suppression des pilotes car le paramètre `PersistAllDeviceInstalls` est défini sur `true` par défaut.

- **Specialize** : la fonctionnalité Plug and Play analyse l'ordinateur et installe les pilotes de tous les périphériques détectés. L'outil génère la configuration requise du système d'exploitation comme le nom de l'ordinateur et le SID. Vous pouvez éventuellement exécuter des commandes dans cette phase.
- **Expérience prête à l'emploi (OOBE)** : le système exécute une version abrégée du programme d'installation de Windows et vous demande de saisir des informations telles que la langue du système, le fuseau horaire et l'organisation enregistrée. Lorsque vous exécutez Sysprep avec EC2Launch v2, le fichier de réponses automatise cette phase.

Actions Sysprep

Sysprep et EC2Launch v2 effectuent les actions suivantes lors de la préparation d'une image.

1. Lorsque vous choisissez Arrêt with Sysprep dans la boîte de dialogue Paramètres de lancement EC2, le système exécute la commande `ec2launch sysprep`.
2. EC2Launch v2 modifie le contenu du fichier `unattend.xml` en lisant la valeur de Registre sur `HKEY_USERS\DEFAULT\Control Panel\International\LocaleName`. Ce fichier se trouve dans le répertoire suivant : `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. Le système exécute `BeforeSysprep.cmd`. Cette commande crée une clé de registre comme suit :

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f
```

La clé de registre désactive les connexions RDP jusqu'à ce qu'elles soient réactivées. La désactivation des connexions RDP est une mesure de sécurité nécessaire, car, au cours de

la première session de démarrage une fois Sysprep exécuté, le protocole RDP autorise les connexions et le mot de passe Administrateur est vide pendant une courte période.

4. Le service EC2Launch v2 appelle Sysprep en exécutant la commande suivante :

```
sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch\nsysprep\unattend.xml"
```

Phase de généralisation

- EC2Launch v2 supprime les informations et les configurations spécifiques à l'image, comme le nom de l'ordinateur et le SID. Si l'instance est membre d'un domaine, elle est supprimée du domaine. Le fichier de réponses `unattend.xml` inclut les paramètres suivants qui affectent cette phase :
 - `PersistAllDeviceInstalls`: ce paramètre empêche le programme d'installation de Windows de supprimer et de reconfigurer des appareils, ce qui accélère le processus de préparation des images, car les AMI Amazon nécessitent certains pilotes pour fonctionner et la redétection de ces pilotes prendrait du temps.
 - `DoNotCleanUpNonPresentAppareils` : ce paramètre conserve les informations Plug-and-Play pour les appareils actuellement absents.
- Sysprep arrête le système d'exploitation au moment où il se prépare à créer l'AMI. Le système lance une nouvelle instance ou démarre l'instance originale.

Phase de spécialisation

Le système génère la configuration requise spécifique au système d'exploitation, comme un nom d'ordinateur et un SID. Le système exécute également les actions suivantes en fonction des configurations que vous spécifiez dans le fichier de réponses `unattend.xml`.

- `CopyProfile`: Sysprep peut être configuré pour supprimer tous les profils utilisateur, y compris le profil administrateur intégré. Ce paramètre conserve le compte d'administrateur intégré afin que les personnalisations que vous effectuez sur ce compte soient transmises à la nouvelle image. La valeur par défaut est `True`.

`CopyProfile` remplace le profil par défaut par le profil d'administrateur local existant. Tous les comptes auxquels vous vous connectez après l'exécution de Sysprep reçoivent une copie de ce profil et de son contenu lors de la première connexion.

Si vous ne disposez pas de personnalisations de profil utilisateur spécifiques que vous souhaitez reporter à la nouvelle image, définissez ce paramètre sur `False`. Sysprep supprime tous les profils utilisateur. Cela permet d'économiser du temps et de l'espace.

- `TimeZone`: le fuseau horaire est défini sur le temps universel coordonné (UTC) par défaut.
- `Synchronous command with order 1` : le système exécute la commande suivante, qui active le compte administrateur et spécifie le mot de passe requis :

```
net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /  
PASSWORDREQ:YES
```

- `Synchronous command with order 2` : le système brouille le mot de passe administrateur. Cette mesure de sécurité est conçue pour empêcher l'accès à l'instance une fois Sysprep terminé si vous n'avez pas configuré la tâche. `setAdminAccount`

Le système exécute la commande suivante depuis le répertoire de votre agent de lancement local (`C:\Program Files\Amazon\EC2Launch\`).

```
EC2Launch.exe internal randomize-password --username Administrator
```

- Pour activer les connexions aux postes de travail à distance, le système définit la clé de `fDenyTSConnections` registre Terminal Server sur `false`.

Phase OOBE

1. Le système spécifie les configurations suivantes à l'aide du fichier de réponses EC2Launch v2 :

- `<InputLocale>en-US</InputLocale>`
- `<SystemLocale>en-US</SystemLocale>`
- `<UILanguage>en-US</UILanguage>`
- `<UserLocale>en-US</UserLocale>`
- `<HideEULAPage>>true</HideEULAPage>`
- `<HideWirelessSetupInOOBE>>true</HideWirelessSetupInOOBE>`
- `<ProtectYourPC>3</ProtectYourPC>`
- `<BluetoothTaskbarIconEnabled>>false</BluetoothTaskbarIconEnabled>`
- `<TimeZone>UTC</TimeZone>`
- `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`

- `<RegisteredOwner>EC2</RegisteredOwner>`

 Note

Pendant les phases de généralisation et de spécialisation, EC2Launch v2 surveille l'état du système d'exploitation. Si EC2Launch v2 détecte que le système d'exploitation est dans une phase Sysprep, il publie le message suivant dans le fichier journal :
Windows est en cours de configuration. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Le système exécute EC2Launch v2.

Étapes post-actions Sysprep

Une fois Sysprep terminé, EC2Launch v2 envoie le message suivant à la sortie de la console :

```
Windows sysprep configuration complete.
```

EC2Launch v2 effectue ensuite les actions suivantes :

1. Lit le contenu du fichier `agent-config.yml` et exécute les tâches configurées.
2. Exécute toutes les tâches de l'étape `preReady`.
3. Une fois qu'il a terminé, envoie un message `Windows is ready` aux journaux du système d'instance.
4. Exécute toutes les tâches de l'étape `PostReady`.

Pour plus d'informations sur EC2Launch v2, consultez [Configurer une instance Windows à l'aide d'EC2Launch v2](#).

Exécution de Sysprep avec EC2Launch v2

Utilisez la procédure suivante pour créer une AMI normalisée à l'aide de Sysprep avec EC2Launch v2.

1. Dans la console Amazon EC2, recherchez l'AMI que vous souhaitez dupliquer.
2. Lancez et connectez-vous à votre instance Windows.
3. Personnalisez-la.

4. Dans le menu Démarrer de Windows, recherchez et choisissez les paramètres Amazon EC2Launch. Pour plus d'informations sur les options et les paramètres de la boîte de dialogue Paramètres Amazon EC2Launch, consultez [Paramètres EC2Launch v2](#).
5. Sélectionnez Arrêter avec Sysprep ou Arrêter sans Sysprep.

Lorsqu'il vous est demandé de confirmer que vous souhaitez exécuter Sysprep et arrêter l'instance, cliquez sur Yes. EC2Launch v2 exécute Sysprep. Ensuite, vous êtes déconnecté de l'instance et l'instance est arrêtée. Si vous consultez la page Instances de la console Amazon EC2, l'état de l'instance passe de Running à Stopping, puis à Stopped. A ce stade, vous pouvez créer une AMI en toute sécurité à partir de cette instance.

Vous pouvez appeler manuellement l'outil Sysprep dans la ligne de commande à l'aide de la commande suivante :

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Utiliser Sysprep avec EC2Launch

EC2Launch offre un fichier de réponse et des fichiers de traitement par lots par défaut pour Sysprep. Ceux-ci permettent d'automatiser et de sécuriser le processus de préparation d'image sur l'AMI. La modification de ces fichiers est facultative. Par défaut, ces fichiers se trouvent dans le répertoire suivant : C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep.

Important

N'utilisez pas Sysprep pour créer une sauvegarde d'instance. Sysprep supprime les informations spécifiques au système. Si vous supprimez ces informations, les conséquences peuvent être néfastes pour une sauvegarde d'instance.

Rubriques Sysprep avec EC2Launch

- [Fichiers de réponses et par lots EC2Launch pour Sysprep](#)
- [Exécuter Sysprep avec EC2Launch](#)
- [Mettre à jour les routes des métadonnées/serveurs KMS pour Server 2016 et versions ultérieures lors du lancement d'une AMI personnalisée](#)

Fichiers de réponses et par lots EC2Launch pour Sysprep

Le fichier de réponse et les fichiers de traitement par lots d'EC2Launch pour Sysprep incluent les éléments suivants :

`Unattend.xml`

Il s'agit du fichier de réponse par défaut. Si vous exécutez `SysprepInstance.ps1` ou choisissez `ShutdownWithSysprep` dans l'interface utilisateur, le système lit le paramètre à partir de ce fichier.

`BeforeSysprep.cmd`

Personnalisez ce fichier de traitement par lots pour exécuter des commandes avant qu'EC2Launch n'exécute Sysprep.

`SysprepSpecialize.cmd`

Personnalisez ce fichier de traitement par lots pour exécuter des commandes au cours de la phase `specialize` de Sysprep.

Exécuter Sysprep avec EC2Launch

Dans l'installation complète de Windows Server 2016 et versions ultérieures (avec un environnement de bureau), vous pouvez exécuter Sysprep avec EC2Launch manuellement ou en utilisant l'application EC2 Launch Settings.

Pour exécuter Sysprep à l'aide de l'application EC2Launch Settings

1. Dans la console Amazon EC2, localisez ou créez une AMI Windows Server 2016 ou ultérieure.
2. Lancez une instance Windows à partir de l'AMI.
3. Connectez-vous à votre instance Windows et personnalisez-la.
4. Recherchez et exécutez l'application EC2LaunchSettings. Par défaut, le fichier se trouve dans le répertoire suivant : `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.

Ec2 Launch Settings

General

Set Computer Name

Set the computer name of the instance ip- <hex internal IP>. Disable this feature to persist your own computer name setting.

Set Wallpaper

Overlay instance information on the current wallpaper.

Extend Boot Volume

Extend OS partition to consume free space for boot volume.

Add DNS Suffix List

Add DNS suffix list to allow DNS resolution of servers running in EC2 without providing the fully qualified domain name.

Handle User Data

Execute user data provided at instance launch.
Note: This will be re-enabled when running shutdown with sysprep below.

Administrator Password

Random (Retrieve from console)

Specify (Temporarily store in config file)

Do Nothing (Customize Unattend.xml for sysprep)

These changes will take effect on next boot if Ec2Launch script is scheduled. By default, it is scheduled by shutdown options below.

Sysprep

Sysprep is a Microsoft tool that prepares an image for multiple launches.

Ec2Launch Script Location: **Found**

Run EC2Launch on every boot (instead of just the next boot).

5. Activez ou désactivez les options au besoin. Ces paramètres sont stockés dans le fichier `LaunchConfig.json`.

6. Pour Mot de passe administrateur, choisissez l'une des options suivantes :
 - Choisissez Random (Aléatoire). EC2Launch génère un mot de passe et le chiffre à l'aide de la clé de l'utilisateur. Le système désactive ce paramètre après le lancement de l'instance afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.
 - Choisissez Specify (Spécifier) et saisissez un mot de passe conforme aux exigences de votre système. Le mot de passe est stocké dans le fichier `LaunchConfig.json` sous forme de texte clair et est supprimé une fois que le mot de passe est défini par Sysprep. Si vous arrêtez maintenant, le mot de passe est défini immédiatement. EC2Launch chiffre le mot de passe à l'aide de la clé de l'utilisateur.
 - Choisissez DoNothinget spécifiez un mot de passe dans le `unattend.xml` fichier. Si vous ne spécifiez pas de mot de passe dans `unattend.xml`, le compte d'administrateur est désactivé.
7. Choisissez Shutdown with Sysprep (Arrêter avec Sysprep).

Pour exécuter manuellement Sysprep via EC2Launch

1. Dans la console Amazon EC2, localisez ou créez une AMI Windows Server 2016 ou ultérieure (édition Datacenter) que vous souhaitez dupliquer.
2. Lancez et connectez-vous à votre instance Windows.
3. Personnalisez l'instance.
4. Spécifiez les paramètres dans le fichier `LaunchConfig.json`. Par défaut, le fichier se trouve dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Pour `adminPasswordType`, spécifiez l'une des valeurs suivantes :

Random

EC2Launch génère un mot de passe et le chiffre à l'aide de la clé de l'utilisateur. Le système désactive ce paramètre après le lancement de l'instance afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.

Specify

EC2Launch utilise le mot de passe que vous spécifiez dans `adminPassword`. Si ce mot de passe ne répond pas aux exigences du système, EC2Launch génère un mot de passe aléatoire à la place. Le mot de passe est stocké dans le fichier `LaunchConfig.json` sous

forme de texte clair et est supprimé une fois que le mot de passe est défini par Sysprep. EC2Launch chiffre le mot de passe à l'aide de la clé de l'utilisateur.

DoNothing

EC2Launch utilise le mot de passe que vous spécifiez dans le fichier `unattend.xml`. Si vous ne spécifiez pas de mot de passe dans `unattend.xml`, le compte d'administrateur est désactivé.

5. (Facultatif) Spécifiez les paramètres dans le fichier `unattend.xml` et autres fichiers de configuration. Si vous prévoyez une installation avec assistance, vous n'avez pas besoin d'apporter des modifications à ces fichiers. Par défaut, les fichiers se trouvent dans le répertoire suivant : `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. Dans Windows PowerShell, exécutez `./InitializeInstance.ps1 -Schedule`. Par défaut, le script se trouve dans le répertoire suivant : `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`. Ce script programme l'instance pour s'initialiser lors du démarrage suivant. Vous devez exécuter ce script avant d'exécuter le script `SysprepInstance.ps1` à l'étape suivante.
7. Dans Windows PowerShell, exécutez `./SysprepInstance.ps1`. Par défaut, le script se trouve dans le répertoire suivant : `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Vous êtes déconnecté de l'instance et l'instance est arrêtée. Si vous consultez la page Instances dans la console Amazon EC2, l'état de l'instance passe de `Running` à `Stopping`, puis à `Stopped`. À ce stade, vous pouvez créer une AMI en toute sécurité à partir de cette instance.

Mettre à jour les routes des métadonnées/serveurs KMS pour Server 2016 et versions ultérieures lors du lancement d'une AMI personnalisée

Pour mettre à jour les routes des métadonnées/serveurs KMS pour Server 2016 et versions ultérieures lors du lancement d'une AMI personnalisée, réalisez l'une des actions suivantes :

- Exécutez l'LaunchSettings interface graphique EC2 (`C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe`) et sélectionnez l'option permettant d'arrêter avec Sysprep.
- Exécutez EC2 LaunchSettings et arrêtez-le sans Sysprep avant de créer l'AMI. Cela configure l'exécution des tâches d'initialisation du lancement EC2 au prochain démarrage, ce qui va définir les routes en fonction du sous-réseau pour l'instance.

- Replanifiez manuellement les tâches d'initialisation d'EC2 Launch avant de créer une AMI à partir de. [PowerShell](#)

Important

Prenez note du comportement de réinitialisation du mot de passe par défaut avant de replanifier les tâches.

- Pour mettre à jour les routes sur une instance en cours d'exécution qui rencontre des échecs d'activation de Windows ou de communication avec les métadonnées de l'instance, consultez [« L'activation de Windows est impossible »](#).

Utiliser Sysprep avec EC2Config

Découvrez en détail les différentes phases d'exécution Sysprep et les tâches exécutées par le service EC2Config à mesure que l'image est préparée. Vous pourrez également consulter les étapes de création d'une AMI normalisée à l'aide de Sysprep avec le service EC2Config.

Rubriques Sysprep avec EC2Config

- [Phases Sysprep](#)
- [Actions Sysprep](#)
- [Étapes post-actions Sysprep](#)
- [Exécution de Sysprep avec le service EC2Config](#)

Phases Sysprep

Sysprep passe par les phases suivantes :

- **Generalize** : l'outil supprime les informations et les configurations spécifiques à l'image. Par exemple, Sysprep supprime l'identificateur de sécurité (SID), le nom de l'ordinateur, les journaux d'événements et des pilotes spécifiques, pour n'en citer que quelques-uns. Une fois cette phase terminée, le système d'exploitation est prêt à créer une AMI.

Note

Lorsque vous exécutez Sysprep avec le service EC2Config, le système empêche la suppression des pilotes car le `PersistAllDeviceInstalls` paramètre est défini sur `true` par défaut.

- **Specialize** : la fonctionnalité Plug and Play analyse l'ordinateur et installe les pilotes de tous les périphériques détectés. L'outil génère la configuration requise du système d'exploitation comme le nom de l'ordinateur et le SID. Vous pouvez éventuellement exécuter des commandes dans cette phase.
- **Out-of-Box Experience (OOBE)** : le système exécute une version abrégée de l'installation Windows et demande à l'utilisateur d'entrer des informations comme la langue du système, le fuseau horaire et une organisation enregistrée. Lorsque vous exécutez Sysprep avec EC2Config, le fichier de réponses automatise cette phase.

Actions Sysprep

Sysprep et le service EC2Config exécutent les actions suivantes lors de la préparation d'une image.

1. Si vous choisissez **Fermeture avec Sysprep** dans la boîte de dialogue **Propriétés du service EC2**, le système exécute la commande `ec2config.exe -sysprep`.
2. Le service EC2Config lit le contenu du fichier `BundleConfig.xml`. Ce fichier se trouve dans le répertoire suivant par défaut : `C:\Program Files\Amazon\Ec2ConfigService\Settings`.

Le fichier `BundleConfig.xml` contient les paramètres suivants. Vous pouvez modifier les paramètres suivants :

- **AutoSysprep**: indique s'il faut utiliser Sysprep automatiquement. Vous n'avez pas besoin de modifier cette valeur si vous exécutez Sysprep dans la boîte de dialogue **EC2 Service Properties**. La valeur par défaut est `No`.
- **SetRDPCertificate** : définit un certificat autosigné pour le serveur des services Bureau à distance. Cela vous permet d'utiliser en toute sécurité le protocole RDP (Remote Desktop Protocol) pour vous connecter à l'instance. Modifiez la valeur sur `Yes` si de nouvelles instances doivent utiliser un certificat. Ce paramètre n'est pas utilisé avec les instances de Windows Server 2012 car ces systèmes d'exploitation peuvent générer leurs propres certificats. La valeur par défaut est `No`.

- `SetPasswordAfterSysprep`: définit un mot de passe aléatoire sur une instance récemment lancée, la chiffre avec la clé de lancement de l'utilisateur et transmet le mot de passe chiffré à la console. Modifiez la valeur sur `No` si de nouvelles instances ne doivent pas être définies sur un mot de passe chiffré aléatoire. La valeur par défaut est `Yes`.
 - `PreSysprepRunCmd`: emplacement de la commande à exécuter. La commande se trouve dans le répertoire suivant, par défaut : `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`
3. Le système exécute `BeforeSysprep.cmd`. Cette commande crée une clé de registre comme suit :

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v  
fDenyTSConnections /t REG_DWORD /d 1 /f
```

La clé de registre désactive les connexions RDP jusqu'à ce qu'elles soient réactivées. La désactivation des connexions RDP est une mesure de sécurité nécessaire, car, au cours de la première session de démarrage une fois `Sysprep` exécuté, le protocole RDP autorise les connexions et le mot de passe Administrateur est vide pendant une courte période.

4. Le service `EC2Config` appelle `Sysprep` en exécutant la commande suivante :

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /  
oobe /generalize /shutdown
```

Phase de généralisation

- L'outil supprime les informations et les configurations spécifiques à l'image, comme le nom de l'ordinateur et le SID. Si l'instance est membre d'un domaine, elle est supprimée du domaine. Le fichier de réponses `sysprep2008.xml` inclut les paramètres suivants qui affectent cette phase :
 - `PersistAllDeviceInstalls`: ce paramètre empêche le programme d'installation de Windows de supprimer et de reconfigurer des appareils, ce qui accélère le processus de préparation des images, car les AMI Amazon nécessitent certains pilotes pour fonctionner et la redétection de ces pilotes prendrait du temps.
 - `DoNotCleanUpNonPresentAppareils` : ce paramètre conserve les informations Plug-and-Play pour les appareils actuellement absents.
- `Sysprep` arrête le système d'exploitation au moment où il se prépare à créer l'AMI. Le système lance une nouvelle instance ou démarre l'instance originale.

Phase de spécialisation

Le système génère la configuration requise spécifique au système d'exploitation, comme un nom d'ordinateur et un SID. Le système exécute également les actions suivantes en fonction des configurations que vous spécifiez dans le fichier de réponses sysprep2008.xml.

- **CopyProfile:** Sysprep peut être configuré pour supprimer tous les profils utilisateur, y compris le profil administrateur intégré. Ce paramètre conserve le compte d'administrateur intégré afin que les personnalisations que vous effectuez sur ce compte soient transmises à la nouvelle image. La valeur par défaut est True.

CopyProfile remplace le profil par défaut par le profil d'administrateur local existant. Tous les comptes qui font l'objet d'une connexion après l'exécution de Sysprep recevront une copie de ce profil et de son contenu lors de la première connexion.

Si vous ne disposez pas de personnalisations de profil utilisateur spécifiques que vous souhaitez reporter à la nouvelle image, définissez ce paramètre sur False. Sysprep supprime tous les profils utilisateur. Cela permet d'économiser du temps et de l'espace.

- **TimeZone:** le fuseau horaire est défini sur le temps universel coordonné (UTC) par défaut.
- **Synchronous command with order 1 :** le système exécute la commande suivante qui active le compte d'administrateur et spécifie l'exigence d'un mot de passe.

```
net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /  
PASSWORDREQ:YES
```

- **Synchronous command with order 2 :** le système brouille le mot de passe administrateur. Cette mesure de sécurité est conçue pour empêcher l'instance d'être accessible une fois que Sysprep se termine si vous n'avez pas activé le paramètre ec2setpassword.

```
Administrateur C:\Program Files \ Amazon \ Ec2 ConfigService \ ScramblePassword .exe » -u
```

- **Synchronous command with order 3 :** le système exécute la commande suivante :

```
C:\Program Files \ Amazon \ Ec2 \ Scripts ConfigService \ Phase.cmd SysprepSpecialize
```

Cette commande ajoute la clé de registre suivante qui réactive le RDP :

```
reg add « HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControl Set \ Control \ Terminal Server » /  
v FdenytsConnections /t REG_DWORD /d 0 /f
```

Phase OOBE

1. A l'aide du fichier de réponses du service EC2Config, le système spécifie les configurations suivantes :

- `< InputLocale InputLocale >fr-FR</ >`
- `< SystemLocale SystemLocale >fr-FR</ >`
- `<UILanguage>en-US</UILanguage>`
- `< UserLocale UserLocale >fr-FR</ >`
- `<HideEULAPage>true</HideEULAPage>`
- `< HideWireless SetupIn OOBE>True</ HideWireless SetupIn OOBE>`
- `< NetworkLocation NetworkLocation >Autres</ >`
- `< ProtectYour PC>3</ PC> ProtectYour`
- `< BluetoothTaskbar IconEnabled BluetoothTaskbar IconEnabled >fauss</ >`
- `< TimeZone TimeZone >UTC</ >`
- `< RegisteredOrganization RegisteredOrganization >Amazon.com</ >`
- `< RegisteredOwner RegisteredOwner >Amazon</ >`

Note

Pendant les phases de généralisation et de spécialisation, le service EC2Config surveille l'état du système d'exploitation. Si le service EC2Config détecte que le système d'exploitation est dans une phase Sysprep, il publie le message suivant dans le fichier journal :

```
ConfigMonitorÉtat EC2 : 0 Windows est en cours de configuration.
```

```
SysprepState=IMAGE_STATE_UNDEPLOYABLE
```

2. Une fois la phase OOBE terminée, le système exécute `SetupComplete.cmd` à partir de l'emplacement suivant : `C:\Windows\Setup\Scripts\SetupComplete.cmd`. Avant avril 2015, dans les AMI publiques Amazon, le fichier était vide et n'exécutait rien sur l'image. Depuis avril 2015, dans les AMI publiques, le fichier comprend la valeur suivante : `call "C:\Program Files\Amazon\Ec2ConfigService\Scripts\PostSysprep.cmd"`.

3. Le système exécute `PostSysprep.cmd`, qui effectue les opérations suivantes :

- Permet de définir que le mot de passe d'administrateur local ne doit pas expirer. Si le mot de passe expirait, les administrateurs ne pourraient pas se connecter.

- Permet de définir le nom de la machine MSSQLServer (le cas échéant) afin que le nom soit synchronisé sur l'AMI.

Étapes post-actions Sysprep

Une fois Sysprep terminé, les services EC2Config envoient le message suivant à la sortie de la console :

```
Windows sysprep configuration complete.  
Message: Sysprep Start  
Message: Sysprep End
```

EC2Config effectue ensuite les actions suivantes :

1. Permet de lire le contenu du fichier config.xml et de répertorier tous les plugins activés.
2. Permet d'exécuter simultanément tous les plugins avant que Windows soit prêt.
 - Eco 2 SetPassword
 - Nom Ec2 SetComputer
 - Eco 2 InitializeDrives
 - Eco 2 EventLog
 - Ec2ConfigureRDP
 - Ec2OutputRDPcert
 - Lettre Ec2 SetDrive
 - Eco 2 WindowsActivate
 - Eco 2 DynamicBoot VolumeSize
3. Une fois terminé, il envoie un message « Windows is ready » aux journaux systèmes de l'instance.
4. Permet d'exécuter simultanément tous les plugins une fois que Windows est prêt.
 - Amazon CloudWatch Logs
 - UserData
 - AWS Systems Manager (Systems Manager)

Pour plus d'informations sur les plugins Windows, consultez [Configuration d'une instance Windows à l'aide du service EC2Config \(ancien\)](#).

Exécution de Sysprep avec le service EC2Config

Utilisez la procédure suivante pour créer une AMI standardisée à l'aide de Sysprep et du service EC2Config.

1. Dans la console Amazon EC2, recherchez ou [créez](#) une AMI que vous souhaitez dupliquer.
2. Lancez et connectez-vous à votre instance Windows.
3. Personnalisez-la.
4. Spécifiez les paramètres de configuration dans le fichier de réponses du service EC2Config :

```
C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml
```

5. Dans le menu Démarrer de Windows, choisissez Tous les programmes, puis sélectionnez ConfigServiceParamètres EC2.
6. Choisissez l'onglet Image dans la boîte de dialogue Ec2 Service Properties. Pour plus d'informations sur les options et les paramètres de la boîte de dialogue Ec2 Service Properties, consultez [Propriétés du service EC2](#).
7. Sélectionnez une option pour le mot de passe de l'administrateur, puis choisissez Shutdown with Sysprep ou Shutdown without Sysprep. EC2Config modifie les fichiers de paramètres en fonction de l'option de mot de passe que vous avez sélectionnée.
 - Random : EC2Config génère un mot de passe, le chiffre avec la clé de l'utilisateur et affiche le mot de passe chiffré sur la console. Nous désactivons ce paramètre après le premier lancement afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.
 - Specify : le mot de passe est stocké dans le fichier de réponses de Sysprep sous une forme chiffrée (texte clair). Lorsque Sysprep s'exécute par la suite, cela définit le mot de passe d'administrateur. Si vous arrêtez maintenant, le mot de passe est défini immédiatement. Lorsque le service redémarre, le mot de passe d'administrateur est supprimé. Il est important de vous rappeler ce mot de passe, car vous ne pourrez pas le récupérer ultérieurement.
 - Keep Existing : le mot de passe existant pour le compte d'administrateur ne change pas lorsque Sysprep est exécuté ou qu'EC2Config est redémarré. Il est important de vous rappeler ce mot de passe, car vous ne pourrez pas le récupérer ultérieurement.
8. Choisissez OK.

Lorsqu'il vous est demandé de confirmer que vous souhaitez exécuter Sysprep et arrêter l'instance, cliquez sur Yes. Vous remarquerez qu'EC2Config exécute Sysprep. Ensuite, vous êtes déconnecté de l'instance, et l'instance est arrêtée. Si vous consultez la page Instances sur la console Amazon

EC2, l'état de l'instance passe de Running à Stopping, puis finalement à Stopped. A ce stade, vous pouvez créer une AMI en toute sécurité à partir de cette instance.

Vous pouvez appeler manuellement l'outil Sysprep dans la ligne de commande à l'aide de la commande suivante :

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep"
```

Note

Les guillemets doubles dans la commande ne sont pas obligatoires si votre shell CMD se trouve déjà dans le répertoire C:\Program Files \ Amazon \ EC2 ConfigService \.

Toutefois, vous devez vérifier que les options de fichier XML spécifiées dans le dossier Ec2ConfigService\Settings sont correctes. Sinon, vous risquez de ne pas pouvoir vous connecter à l'instance. Pour plus d'informations sur les fichiers de paramètres, consultez [Fichiers de paramètres EC2Config](#). Pour obtenir un exemple de configuration, puis d'exécution de Sysprep depuis la ligne de commande, consultez Ec2ConfigService\Scripts\InstallUpdates.ps1.

Modification d'une AMI

Vous pouvez modifier un ensemble limité d'attributs d'Amazon Machine Image (AMI), tels que la description et les propriétés de partage de l'AMI. Toutefois, le contenu d'AMI (données binaires du volume) ne peut pas être modifié. Pour modifier le contenu de l'AMI, vous devez [créer une nouvelle AMI](#).

Important

Vous ne pouvez pas modifier le contenu (données binaires du volume) d'une AMI basée sur EBS, car les instantanés sur lesquels les données reposent sont immuables. Vous ne pouvez pas non plus modifier le contenu (données binaires de volume) d'une AMI Linux stockée (basée sur S3) d'une instance, car le contenu est signé et les lancements d'instances échoueront si les signatures ne correspondent pas.

Pour connaître les attributs de l'AMI qui peuvent être modifiés, consultez la section [ModifyImageAttribut](#) du manuel Amazon EC2 API Reference.

Les rubriques suivantes fournissent des instructions pour utiliser la console Amazon EC2 et AWS CLI pour modifier les attributs d'une AMI :

- [Rendre une AMI publique](#)
- [Partager une AMI avec des organisations ou des unités d'organisations spécifiques](#)
- [Partager une AMI avec des comptes AWS spécifiques](#)
- [Utiliser le support payant](#)
- [Configurer l'AMI](#)

Copier une AMI

Vous pouvez copier une Amazon Machine Image (AMI) au sein d'une région ou d'une AWS région à l'autre. Vous pouvez copier à la fois des AMI basées sur Amazon EBS et des AMI basées sur le stockage d'instance. Vous pouvez copier des AMI basées sur EBS avec des instantanés chiffrés et également modifier l'état du chiffrement pendant le processus de copie. Vous pouvez copier les AMI partagées avec vous.

La copie d'une AMI source produit une nouvelle AMI identique mais distincte, également appelée AMI cible. L'AMI cible possède son propre ID d'AMI unique. Vous pouvez modifier ou annuler l'enregistrement d'une AMI source sans que cela ait un impact sur l'AMI cible. L'inverse est également vrai.

Avec une AMI basée sur EBS, chacun de ses instantanés de sauvegarde est copié sur un instantané cible identique mais distinct. Si vous copiez une AMI dans une nouvelle région, les instantanés sont des copies complètes (non incrémentielles). Si vous chiffrez des instantanés de sauvegarde non chiffrés ou si vous les chiffrez sur une nouvelle clé KMS, les instantanés sont des copies complètes (non incrémentielles). Les opérations de copie suivantes d'une AMI créent des copies incrémentielles des instantanés de sauvegarde.

Table des matières

- [Considérations](#)
- [Coûts](#)
- [Autorisations IAM](#)
- [Copier une AMI](#)
- [Arrêter la copie d'une AMI en attente](#)
- [Copie entre régions](#)

- [Copie entre comptes](#)
- [Chiffrement et copie](#)

Considérations

- Autorisation de copier des AMI : vous pouvez utiliser des politiques IAM pour accorder ou refuser aux utilisateurs l'autorisation de copier des AMI. Les autorisations de niveau ressource spécifiées pour l'action CopyImage s'appliquent uniquement à la nouvelle AMI. Vous ne pouvez pas spécifier d'autorisations au niveau des ressources pour l'AMI source.
- Autorisations de lancement et autorisations de compartiment Amazon S3 : AWS ne copie pas les autorisations de lancement ou les autorisations de compartiment Amazon S3 de l'AMI source vers la nouvelle AMI. Une fois la copie terminée, vous pouvez appliquer les autorisations de lancement et les permissions de compartiment Amazon S3 à la nouvelle AMI.
- Balises : vous ne pouvez copier que les balises AMI définies par l'utilisateur que vous avez jointes à l'AMI source. Les balises système (préfixées par aws :) et les balises qdéfinies par l'utilisateur qui sont attachées par d'autres Comptes AWS ne seront pas copiées. Lorsque vous copiez une AMI, vous pouvez associer de nouvelles balises à l'AMI cible et à ses instantanés de sauvegarde.

Coûts

Vous n'êtes pas facturé pour la copie d'une AMI. Toutefois, les taux standard de stockage et de transfert de données s'appliquent. Si vous copiez une AMI basée sur EBS, des frais seront facturés pour le stockage de tout instantané EBS supplémentaire.

Autorisations IAM

Pour copier une AMI basée sur EBS ou une instance store-backed, vous devez disposer des autorisations IAM suivantes :

- `ec2:CopyImage`— Pour copier l'AMI. Pour les AMI basées sur EBS, il autorise également la copie des instantanés de sauvegarde de l'AMI.
- `ec2:CreateTags`— Pour baliser l'AMI cible. Pour les AMI basées sur EBS, il autorise également à baliser les instantanés de sauvegarde de l'AMI cible.

Si vous copiez une AMI sauvegardée par instance, vous avez besoin des autorisations IAM supplémentaires suivantes :

- `s3:CreateBucket`— Pour créer le compartiment S3 dans la région cible pour la nouvelle AMI
- `s3:GetBucketAcl`— Pour lire les autorisations ACL pour le bucket source
- `s3:ListAllMyBuckets`— Pour trouver un compartiment S3 existant pour les AMI dans la région cible
- `s3:GetObject`— Pour lire les objets du bucket source
- `s3:PutObject`— Pour écrire les objets dans le compartiment cible
- `s3:PutObjectAcl`— Pour écrire les autorisations pour les nouveaux objets dans le compartiment cible

Exemple de politique IAM pour copier une AMI basée sur EBS et baliser l'AMI cible et les instantanés

L'exemple de politique suivant vous autorise à copier n'importe quelle AMI basée sur EBS et à étiqueter l'AMI cible et ses instantanés de sauvegarde.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "PermissionToCopyAllImages",
    "Effect": "Allow",
    "Action": [
      "ec2:CopyImage",
      "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:*::image/*"
  ]
}
```

Exemple de politique IAM pour copier une AMI basée sur EBS mais refuser de baliser les nouveaux instantanés

L'`ec2:CopySnapshot` autorisation est automatiquement accordée lorsque vous l'`ec2:CopyImage` obtenez. Cela inclut l'autorisation de baliser les nouveaux instantanés de sauvegarde de l'AMI cible. L'autorisation de baliser les nouveaux instantanés de sauvegarde peut être explicitement refusée.

L'exemple de politique suivant vous autorise à copier n'importe quelle AMI basée sur EBS, mais vous interdit de baliser les nouveaux instantanés de sauvegarde de l'AMI cible.

```
{
```

```

"Version": "2012-10-17",
"Statement": [{
  "Effect": "Allow",
  "Action": [
    "ec2:CopyImage",
    "ec2:CreateTags"
  ],
  "Resource": "arn:aws:ec2:*::image/*"
},
{
  "Effect": "Deny",
  "Action": "ec2:CreateTags",
  "Resource": "arn:aws:ec2::*:snapshot/*"
}
]
}

```

Exemple de politique IAM pour copier une AMI sauvegardée par une instance store-back et baliser l'AMI cible

L'exemple de politique suivant vous autorise à copier toute AMI sauvegardée en instance dans le compartiment source spécifié vers la région spécifiée et à étiqueter l'AMI cible.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "PermissionToCopyAllImages",
    "Effect": "Allow",
    "Action": [
      "ec2:CopyImage",
      "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:*::image/*"
  },
  {
    "Effect": "Allow",
    "Action": "s3:ListAllMyBuckets",
    "Resource": [
      "arn:aws:s3::*:"
    ]
  },
  {
    "Effect": "Allow",

```

```
    "Action": "s3:GetObject",
    "Resource": [
      "arn:aws:s3:::ami-source-bucket/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:GetBucketAcl",
      "s3:PutObjectAcl",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::amis-for-account-in-region-hash"
    ]
  }
]
```

Pour trouver le Amazon Resource Name (ARN) du compartiment source de l'AMI, ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>, puis choisissez AMI dans le panneau de navigation et recherchez le nom du compartiment dans la colonne Source.

Note

L'`s3:CreateBucket` autorisation n'est requise que la première fois que vous copiez une AMI sauvegardée par une instance store-backed dans une région spécifique. Après cela, le compartiment Amazon S3 qui est déjà créé dans la région est utilisé pour stocker tous les futurs AMIs que vous copiez dans cette région.

Copier une AMI

Vous pouvez copier une AMI à l'AWS Management Console aide de l'AWS Command Line Interface API Amazon EC2 ou des SDK, qui prennent tous en charge CopyImage l'action.

Console

Pour copier une AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans la barre de navigation de la console, sélectionnez la région comportant l'AMI.
3. Dans le volet de navigation, choisissez AMIs pour afficher la liste des AMI disponibles dans la région.
4. Si l'AMI que vous souhaitez copier ne s'affiche pas, choisissez un autre filtre. Vous pouvez filtrer en fonction des AMI que je possède, des images privées, des images publiques et des images désactivées.
5. Sélectionnez l'AMI à copier, puis choisissez Actions, Copier l'AMI.
6. Sur la page Copy AMI (Copier une AMI), spécifiez les informations suivantes :
 - a. AMI copy name (Nom de la copie de l'AMI) : un nom pour la nouvelle AMI. Vous pouvez inclure les informations relatives au système d'exploitation dans le nom, car Amazon EC2 ne fournit pas ces informations lors de l'affichage des informations relatives à l'AMI.
 - b. AMI copy description (Description de la copie de l'AMI) : par défaut, la description inclut des informations sur l'AMI source afin que vous puissiez distinguer la copie de l'original. Vous pouvez modifier cette description si nécessaire.
 - c. Région de destination : région dans laquelle vous souhaitez copier l'AMI. Pour plus d'informations, consultez [Copie entre régions](#).
 - d. Copier les balises : cochez cette case pour inclure les balises d'AMI définies par l'utilisateur lors de la copie de l'AMI. Les balises système (préfixées par aws :) et les balises qdéfinies par l'utilisateur qui sont attachées par d'autres Comptes AWS ne seront pas copiées.
 - e. (AMI basées sur EBS uniquement) Chiffrer les instantanés EBS de la copie de l'AMI : cochez cette case pour chiffrer les instantanés cibles ou pour les rechiffrer à l'aide d'une autre clé. Si le chiffrement est activé par défaut, la case Chiffrer les instantanés EBS de la copie AMI est cochée et ne peut pas être désactivée. Pour plus d'informations, consultez [Chiffrement et copie](#).
 - f. (AMI basées sur EBS uniquement) Clé KMS : clé KMS à utiliser pour chiffrer les instantanés cibles.
 - g. Balises : vous pouvez étiqueter la nouvelle AMI et les nouveaux instantanés avec les mêmes balises, ou vous pouvez les étiqueter avec des balises différentes.
 - Pour étiqueter la nouvelle AMI et les nouveaux instantanés avec les mêmes balises, choisissez Marquer ensemble l'image et les instantanés. Les mêmes balises sont appliquées à la nouvelle AMI et à chaque instantané créé.

- Pour étiqueter la nouvelle AMI et les nouveaux instantanés avec des balises différentes, choisissez Marquer l'image et les instantanés séparément. Différentes balises sont appliquées à la nouvelle AMI et aux instantanés créés. Notez toutefois que tous les nouveaux instantanés créés reçoivent les mêmes balises ; vous ne pouvez pas étiqueter chaque nouvel instantané avec une balise différente.

(Facultatif) Pour ajouter une balise, sélectionnez Add tag (Ajouter une balise) et saisissez la clé et la valeur de la balise. Répétez l'opération pour chaque étiquette.

- h. Lorsque vous êtes prêt à copier l'AMI, choisissez Copier l'AMI.

L'état initial de la nouvelle AMI est Pending. L'opération de copie AMI est terminée lorsque l'état passe à Available.

AWS CLI

Pour copier une AMI à l'aide du AWS CLI

Vous pouvez copier une AMI à l'aide de la commande [copy-image](#). Vous devez indiquer les régions source et de destination. Vous spécifiez la région source à l'aide du paramètre `--source-region`. Vous pouvez spécifier la région de destination à l'aide du paramètre `--region` ou d'une variable d'environnement. Pour plus d'informations, voir [Configuration de l'interface de ligne de AWS commande](#).

(AMI basées sur EBS uniquement) Lorsque vous chiffrez un instantané cible pendant la copie, vous devez spécifier les paramètres supplémentaires suivants : `et. --encrypted --kms-key-id`

Pour des exemples de commandes, veuillez consulter les [exemples](#) sous [copy-image](#) dans la référence des commandes AWS CLI .

PowerShell

Pour copier une AMI à l'aide des outils pour Windows PowerShell

Vous pouvez copier une AMI à l'aide de la [Copy-EC2Image](#) commande. Vous devez indiquer les régions source et de destination. Vous spécifiez la région source à l'aide du paramètre `-SourceRegion`. Vous pouvez spécifier la région de destination à l'aide du paramètre `-Region` ou de la commande `Set-AWSDefaultRegion`. Pour plus d'informations, consultez la section [Spécification AWS des régions](#).

(AMI basées sur EBS uniquement) Lorsque vous chiffrez un instantané cible pendant la copie, vous devez spécifier les paramètres supplémentaires suivants : `et. -Encrypted -KmsKeyId`

Arrêter la copie d'une AMI en attente

Vous pouvez arrêter une copie d'AMI en attente à l'aide de la ligne de commande AWS Management Console ou de la ligne de commande.

Console

Pour arrêter l'opération de copie d'une AMI à l'aide de la console

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région de destination dans le sélecteur de régions.
3. Dans le panneau de navigation, sélectionnez AMI.
4. Sélectionnez l'AMI pour arrêter la copie, puis choisissez Actions, Désenregistrer l'AMI.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Deregister AMI (Annuler l'enregistrement de l'AMI).

Command line

Pour arrêter une opération de copie d'une AMI à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [deregister-image](#) (AWS CLI)
- [Unregister-EC2Image](#) (AWS Tools for Windows PowerShell)

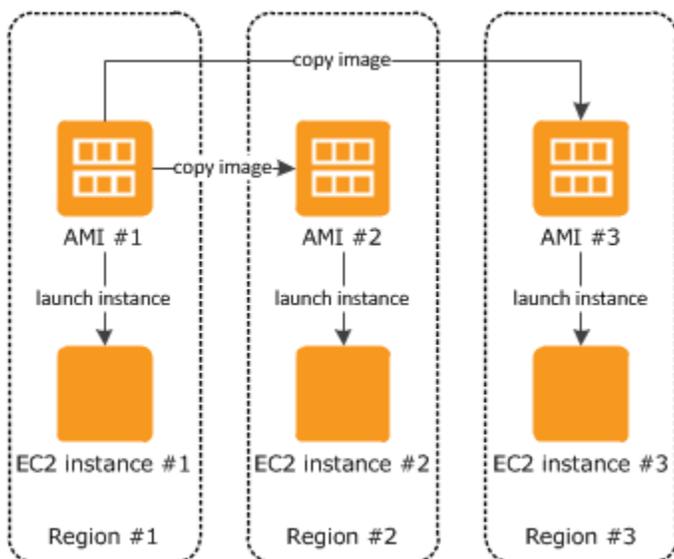
Copie entre régions

La copie d'une AMI entre différentes régions géographiques offre les avantages suivants :

- Déploiement international uniforme : la copie d'une AMI d'une région à l'autre vous permet de lancer des instances uniformes reposant sur la même AMI dans différentes régions.

- **Évolutivité** : vous pouvez plus facilement concevoir et créer des applications d'envergure internationale répondant aux besoins de vos utilisateurs, quel que soit l'emplacement.
- **Performances** : vous pouvez accroître les performances en distribuant votre application, ainsi qu'en recherchant les composants critiques de votre application plus près de vos utilisateurs. Vous pouvez également tirer parti des fonctionnalités spécifiques à la région, telles que les types d'instances ou d'autres AWS services.
- **Disponibilité élevée** : vous pouvez concevoir et déployer des applications dans différentes régions AWS afin d'accroître leur disponibilité.

Le schéma suivant montre la relation entre une AMI source et deux AMI copiées dans différentes régions, ainsi que les instances EC2 lancées depuis chacune d'elles. Lorsque vous lancez une instance à partir d'une AMI, elle se trouve dans la même région que l'AMI. Si vous modifiez l'AMI source et que vous souhaitez faire apparaître ces modifications dans les AMIs des régions cibles, vous devez recopier l'AMI source dans les régions cibles.



La première fois que vous copiez une AMI basée sur le stockage d'instance dans une région, nous créons un compartiment Amazon S3 pour les AMIs copiées dans cette région. Toutes les AMIs basées sur le stockage d'instance que vous copiez dans cette région sont stockées dans ce compartiment. Les noms des compartiments ont le format suivant : amis-for-*account*-in-*region-hash*. Par exemple : amis-for-123456789012-in-us-east-2-yhjmxvp6.

Prérequis

Avant de copier une AMI, vous devez veiller à ce que le contenu de l'AMI source ait été mis à jour afin de pouvoir être exécuté dans une région différente. Par exemple, vous devez mettre à jour

toutes les chaînes de connexion à la base de données ou des données de configuration d'application similaires de façon à ce qu'elles pointent vers les ressources appropriées. Dans le cas contraire, les instances lancées depuis la nouvelle AMI dans la région de destination peuvent toujours utiliser les ressources de la région source, ce qui peut avoir un impact sur les performances et les coûts.

Limites

- Les régions de destination sont limitées à 100 copies d'une AMI à la fois.
- Vous ne pouvez pas copier une AMI paravirtuelle (PV) dans une région qui ne prend pas en charge les AMI PV. Pour plus d'informations, consultez [Types de virtualisation AMI](#).

Copie entre comptes

Vous pouvez partager une AMI avec un autre AWS compte. Le partage d'une AMI n'affecte pas la propriété de celle-ci. Le compte propriétaire est facturé pour le stockage dans la région. Pour plus d'informations, consultez [Partager une AMI avec des comptes AWS spécifiques](#).

Si vous copiez une AMI qui a été partagée avec votre compte, vous êtes le propriétaire de l'AMI cible de votre compte. Le propriétaire de l'AMI source se voit facturer des frais standard de transfert Amazon EBS ou Amazon S3, et vous devez régler le stockage de l'AMI cible dans la région de destination.

Autorisations d'accès aux ressources

Pour copier une AMI qui a été partagée avec vous à partir d'un autre compte, le propriétaire de l'AMI source doit vous accorder des autorisations de lecture pour le stockage sur lequel est basée l'AMI. Le stockage est soit l'instantané EBS associé (pour une AMI basée sur Amazon EBS) soit un compartiment S3 associé (pour une AMI basée sur le stockage d'instances). Si l'AMI partagée comporte des instantanés chiffrés, le propriétaire doit également partager la ou les clé(s) avec vous. Pour plus d'informations sur l'octroi d'autorisations de ressources, pour les instantanés EBS, voir [Partager un instantané Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS, et pour les compartiments S3, voir Gestion des [identités et des accès dans Amazon S3 dans](#) le guide de l'utilisateur d'Amazon Simple Storage Service.

Note

Pour copier une AMI avec ses balises, vous devez disposer des autorisations de lancement pour l'AMI source.

Chiffrement et copie

Le tableau suivant représente la prise en charge du chiffrement dans divers cas de figure de copie d'AMI. Bien qu'il soit possible de copier un instantané non chiffré pour créer un instantané chiffré, vous ne pouvez pas copier un instantané chiffré et en créer un qui ne soit pas chiffré.

Scénario	Description	Pris en charge
1	Non chiffré vers non chiffré	Oui
2	Chiffré vers chiffré	Oui
3	Non chiffré vers chiffré	Oui
4	Chiffré vers non chiffré	Non

Note

Le chiffrement pendant l'action CopyImage s'applique uniquement aux AMIs basées sur Amazon EBS. Dans la mesure où une AMI basée sur le stockage d'instance ne s'appuie pas sur les instantanés, vous ne pouvez pas utiliser la copie pour modifier son statut de chiffrement.

Par défaut (à savoir, sans spécifier les paramètres de chiffrement), l'instantané sur lequel repose une AMI est copié avec son statut de chiffrement initial. La copie d'une AMI reposant sur un instantané non chiffré crée un instantané cible identique qui n'est pas chiffré non plus. Si l'AMI source est soutenue par un instantané chiffré, sa copie permet d'obtenir un instantané cible identique chiffré par la même AWS KMS clé. La copie d'une AMI basée sur plusieurs instantanés conserve, par défaut, le statut de chiffrement source dans chaque instantané cible.

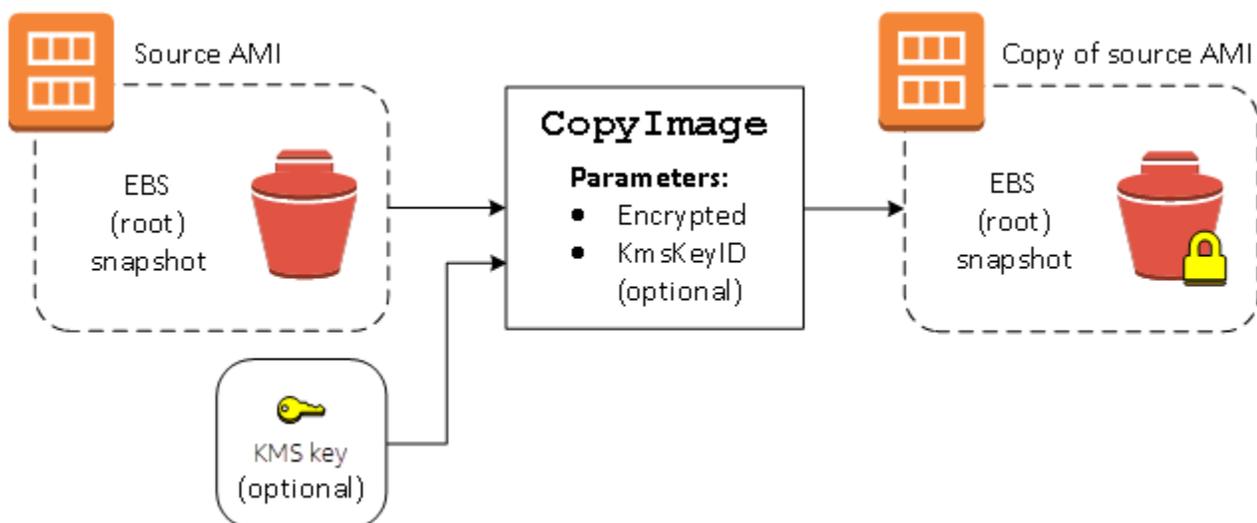
Si vous spécifiez les paramètres de chiffrement lors de la copie d'une AMI, vous pouvez chiffrer ou re-chiffrer ses instantanés. L'exemple suivant montre un cas (non par défaut) qui fournit les paramètres de chiffrement à l'action CopyImage dans le but de modifier l'état de chiffrement de l'AMI cible.

Copier une AMI source non chiffrée vers une AMI cible chiffrée

Dans ce scénario, une AMI basée sur un instantané racine non chiffré est copiée sur une AMI avec un instantané racine chiffré. L'action `CopyImage` est appelée avec deux paramètres de chiffrement, y compris une clé gérée par le client. Par conséquent, l'état de chiffrement de l'instantané racine change, de sorte que l'AMI cible est basée sur un instantané racine contenant les mêmes données que l'instantané source, mais chiffrée à l'aide de la clé spécifiée. Vous supportez des coûts de stockage pour les instantanés dans les deux AMI, ainsi que des frais pour toutes les instances que vous lancez à partir de l'une ou l'autre AMI.

Note

L'activation du chiffrement par défaut a le même effet que la définition du `Encrypted` paramètre sur `true` pour tous les instantanés de l'AMI.



Définir le paramètre `Encrypted` chiffre l'instantané unique de cette instance. Si vous ne spécifiez pas le paramètre `KmsKeyId`, la clé gérée par le client par défaut est utilisée pour chiffrer la copie de l'instantané.

Pour plus d'informations sur la copie d'AMIs avec des instantanés chiffrés, consultez [Utiliser le chiffrement avec des AMI basées sur EBS](#).

Stocker et restaurer une AMI à l'aide de S3

Vous pouvez stocker une Amazon Machine Image (AMI) dans un compartiment Amazon S3, copier l'AMI dans un autre compartiment S3, puis la restaurer à partir du compartiment S3. En stockant et en restaurant une AMI à l'aide de compartiments S3, vous pouvez copier des AMI d'une AWS

partition à une autre, par exemple de la partition commerciale principale vers la AWS GovCloud (US) partition. Vous pouvez également effectuer des copies d'archivage des AMI en les stockant dans un compartiment S3.

Les API prises en charge pour le stockage et la restauration d'une AMI à l'aide de S3 sont `CreateStoreImageTask`, `DescribeStoreImageTasks` et `CreateRestoreImageTask`.

`CopyImage` est l'API recommandée pour copier des AMI au sein d'une AWS partition. Toutefois, `CopyImage` ne peut pas copier une AMI vers une autre partition.

Pour plus d'informations sur les AWS partitions, consultez la section *partition* sur la page [Amazon Resource Names \(ARNs\)](#) du guide de l'utilisateur IAM.

Warning

Assurez-vous de respecter toutes les lois et exigences commerciales applicables lorsque vous déplacez des données entre des AWS partitions ou des AWS régions, y compris, mais sans s'y limiter, les réglementations gouvernementales applicables et les exigences en matière de résidence des données.

Rubriques

- [Cas d'utilisation](#)
- [Fonctionnement des API de stockage et de restauration de l'AMI](#)
- [Limites](#)
- [Coûts](#)
- [Sécurisation de vos AMI](#)
- [Autorisations de stockage et de restauration des AMI à l'aide de S3](#)
- [Utilisation des API de stockage et de restauration des AMI](#)
- [Utilisation de chemins d'accès aux fichiers dans S3](#)

Cas d'utilisation

Utilisez les API de stockage et de restauration pour effectuer les opérations suivantes :

- [Copier une AMI d'une AWS partition vers une autre AWS](#)
- [Faire des copies d'archivage des AMI](#)

Copier une AMI d'une AWS partition vers une autre AWS

En stockant et en restaurant une AMI à l'aide de compartiments S3, vous pouvez copier une AMI d'une AWS partition à une autre ou d'une AWS région à une autre. Dans l'exemple suivant, vous copiez une AMI de la partition commerciale principale vers la AWS GovCloud (US) partition, en particulier de la us-east-2 région vers la us-gov-east-1 région.

Pour copier une AMI d'une partition dans une autre, procédez comme suit :

- Stockez l'AMI dans un compartiment S3 dans la région actuelle à l'aide de `CreateStoreImageTask`. Dans cet exemple, le compartiment S3 se trouve dans us-east-2. Pour obtenir un exemple de commande, consultez [Stocker une AMI dans un compartiment S3](#).
- Surveillez la progression de la tâche de stockage à l'aide de `DescribeStoreImageTasks`. L'objet devient visible dans le compartiment S3 lorsque la tâche est terminée. Pour obtenir un exemple de commande, consultez [Décrire la progression d'une tâche de stockage d'AMI](#).
- Copiez l'objet AMI stocké dans un compartiment S3 de la partition cible à l'aide d'une procédure de votre choix. Dans cet exemple, le compartiment S3 se trouve dans us-gov-east-1.

Note

Comme vous avez besoin AWS d'informations d'identification différentes pour chaque partition, vous ne pouvez pas copier un objet S3 directement d'une partition à l'autre. Le processus de copie d'un objet S3 d'une partition vers une autre n'entre pas dans le cadre de cette documentation. Les processus de copie suivants sont fournis à titre d'exemple uniquement. N'hésitez pas à utiliser celui qui répond le mieux à vos exigences de sécurité.

- Pour copier une AMI d'une partition vers une autre, procédez simplement comme suit : [téléchargez l'objet](#) à partir du compartiment source vers un hôte intermédiaire (par exemple, une instance EC2 ou un ordinateur portable), puis [chargez l'objet](#) depuis l'hôte intermédiaire vers le compartiment cible. Pour chaque étape du processus, utilisez les AWS informations d'identification de la partition.
 - Pour une utilisation plus soutenue, n'hésitez pas à développer une application permettant de gérer les copies, en utilisant éventuellement des [téléchargements et des chargements partitionnés S3](#).
- Restaurez l'AMI à partir du compartiment S3 dans la partition cible à l'aide de `CreateRestoreImageTask`. Dans cet exemple, le compartiment S3 se trouve dans us-gov-

east -1. Pour obtenir un exemple de commande, consultez [Restaurer une AMI à partir d'un compartiment S3](#).

- Surveillez la progression de la tâche de restauration en décrivant l'AMI pour vérifier quand son état devient disponible. Vous pouvez également surveiller les pourcentages de progression des instantanés qui composent l'AMI restaurée en décrivant les instantanés.

Faire des copies d'archivage des AMI

Vous pouvez faire des copies d'archivage des AMI en les stockant dans un compartiment S3. Pour obtenir un exemple de commande, consultez [Stocker une AMI dans un compartiment S3](#).

L'AMI est compressée dans un seul objet dans S3. Toutes les métadonnées AMI (à l'exclusion des informations de partage) sont conservées dans le cadre de l'AMI stockée. Les données d'AMI sont compressées dans le cadre du processus de stockage. Les AMI qui contiennent des données qui peuvent être facilement compressées prennent moins de place dans S3. Pour réduire les coûts, vous pouvez utiliser des niveaux de stockage S3 moins onéreux. Pour plus d'informations, consultez [Classes de stockage Amazon S3](#) et les [tarifs Amazon S3](#)

Fonctionnement des API de stockage et de restauration de l'AMI

Pour stocker et restaurer une AMI à l'aide de S3, utilisez les API suivantes :

- `CreateStoreImageTask` – Stocke l'AMI dans un compartiment S3
- `DescribeStoreImageTasks` – Fournit la progression de la tâche de stockage de l'AMI
- `CreateRestoreImageTask` – Restaure l'AMI à partir d'un compartiment S3

Fonctionnement des API

- [CreateStoreImageTask](#)
- [DescribeStoreImageTasks](#)
- [CreateRestoreImageTask](#)

CreateStoreImageTask

L'[CreateStoreImageTask](#) API stocke une AMI sous la forme d'un objet unique dans un compartiment S3.

L'API crée une tâche qui lit toutes les données de l'AMI et de ses instantanés, puis utilise un [chargement partitionné S3](#) pour stocker les données dans un objet S3. L'API prend tous les composants de l'AMI, y compris la plupart des métadonnées AMI non spécifiques à la région, et tous les instantanés EBS contenus dans l'AMI, puis les réunit dans un seul objet dans S3. Les données sont compressées dans le cadre du processus de chargement afin de réduire la quantité d'espace utilisé dans S3, de sorte que la taille de l'objet dans S3 peut être inférieure à la somme des tailles des instantanés dans l'AMI.

Si des balises d'AMI et d'instantanés sont visibles pour le compte appelant cette API, elles sont conservées.

L'objet dans S3 possède le même ID que l'AMI, mais avec une extension `.bin`. Les données suivantes sont également stockées en tant que balises de métadonnées S3 sur l'objet S3 : nom de l'AMI, description de l'AMI, date d'enregistrement de l'AMI, compte propriétaire de l'AMI et horodatage pour l'opération de stockage.

Le temps nécessaire à l'exécution de la tâche dépend de la taille de l'AMI. Il dépend également du nombre d'autres tâches en cours car les tâches sont mises en file d'attente. Vous pouvez suivre la progression de la tâche en appelant l'[DescribeStoreImageTasks](#)API.

La somme des tailles de toutes les AMI en cours est limitée à 600 Go de données instantanées EBS par compte. La création d'autres tâches est rejetée jusqu'à ce que les tâches en cours soient inférieures à la limite. Par exemple, si une AMI contenant 100 Go de données d'instantanés et une autre AMI contenant 200 Go de données d'instantanés sont actuellement stockées, une autre demande est acceptée, car le total en cours de 300 Go est inférieur à la limite. Mais si une seule AMI contenant 800 Go de données d'instantanés est actuellement stockée, les autres tâches sont rejetées jusqu'à ce que la tâche soit terminée.

DescribeStoreImageTasks

L'[DescribeStoreImageTasks](#)API décrit la progression des tâches du magasin AMI. Vous pouvez décrire les tâches des AMI spécifiées. Si vous ne spécifiez pas d'AMI, vous obtenez une liste paginée de toutes les tâches d'image de stockage traitées au cours des 31 derniers jours.

Pour chaque tâche AMI, la réponse indique si la tâche est `InProgress`, `Completed` ou `Failed`. Pour les tâches `InProgress`, la réponse affiche une progression estimée en pourcentage.

Les tâches sont répertoriées dans l'ordre chronologique inverse.

Actuellement, seules les tâches du mois précédent peuvent être affichées.

CreateRestoreImageTask

L'[CreateRestoreImageTask](#) API lance une tâche qui restaure une AMI à partir d'un objet S3 précédemment créé à l'aide d'une [CreateStoreImageTask](#) demande.

La tâche de restauration peut être exécutée dans la même région ou dans une autre région dans laquelle la tâche de stockage a été réalisée.

Le compartiment S3 à partir duquel l'objet AMI est restauré doit se trouver dans la même région que celle dans laquelle la tâche de restauration est demandée. L'AMI est restaurée dans cette région.

L'AMI est restaurée avec ses métadonnées, telles que le nom, la description et les mappages de périphériques de stockage en mode bloc correspondant aux valeurs de l'AMI stockée. Le nom doit être unique pour les AMI de la région pour ce compte. Si vous n'indiquez pas de nom, la nouvelle AMI reçoit le même nom que l'AMI d'origine. L'AMI obtient un nouvel ID d'AMI qui est généré lors du processus de restauration.

Le temps nécessaire pour terminer la tâche de restauration de l'AMI dépend de la taille de l'AMI. Il dépend également du nombre d'autres tâches en cours car les tâches sont mises en file d'attente. Vous pouvez afficher la progression de la tâche en décrivant l'AMI ([describe-images](#)) ou ses instantanés EBS ([describe-snapshots](#)). Si la tâche échoue, l'AMI et les instantanés basculent en état d'échec.

La somme des tailles de toutes les AMI en cours est limitée à 300 Go (en fonction de la taille après restauration) de données d'instantanés EBS par compte. La création d'autres tâches est rejetée jusqu'à ce que les tâches en cours soient inférieures à la limite.

Limites

- Pour stocker une AMI, votre Compte AWS devez soit être propriétaire de l'AMI et de ses instantanés, soit [partager l'AMI et ses instantanés directement avec votre compte](#). Vous ne pouvez pas stocker une AMI si elle est uniquement [partagée publiquement](#).
- Seules les AMI basées sur EBS peuvent être stockées à l'aide de ces API.
- Les AMI paravirtuelles (PV) ne sont pas prises en charge.
- La taille d'une AMI (avant compression) pouvant être stockée est limitée à 5 000 Go.
- Quota sur les demandes [d'image de stockage](#) : tâche de stockage de 600 Go (données instantanées) en cours.
- Quota sur les demandes [d'image de restauration](#) : tâche de restauration de 300 Go (données d'instantanés) en cours.

- Pendant la durée de la tâche de stockage, les instantanés ne doivent pas être supprimés et le principal IAM qui effectue le stockage doit avoir accès aux instantanés. Dans le cas contraire, le processus de stockage échoue.
- Vous ne pouvez pas créer plusieurs copies d'une AMI dans le même compartiment S3.
- Une AMI stockée dans un compartiment S3 ne peut pas être restaurée avec son ID d'AMI d'origine. Pour pallier à cela, vous pouvez utiliser l'[alias de l'AMI](#).
- Actuellement, les API de stockage et de restauration ne sont prises en charge qu'à l'AWS Command Line Interface aide AWS des SDK et de l'API Amazon EC2. Vous ne pouvez pas stocker et restaurer une AMI à l'aide de la console Amazon EC2.

Coûts

Lorsque vous stockez et restaurez des AMI à l'aide de S3, vous êtes facturé pour les services qui sont utilisés par les API de stockage et de restauration, ainsi que pour le transfert de données. Les API utilisent S3 et l'API directe EBS (utilisée en interne par ces API pour accéder aux données d'instantanés). Pour en savoir plus, consultez les [tarifs Amazon S3](#) et les [tarifs Amazon EBS](#).

Sécurisation de vos AMI

Pour utiliser les API de stockage et de restauration, le compartiment S3 et l'AMI doivent se trouver dans la même région. Assurez-vous que la sécurité configurée pour le compartiment S3 est suffisante pour sécuriser le contenu de l'AMI et qu'elle sera assurée aussi longtemps que les objets de l'AMI resteront dans le compartiment. Si cela ne peut pas être fait, l'utilisation de ces API n'est pas recommandée. Assurez-vous qu'aucun accès public au compartiment S3 n'est autorisé. Même si cela n'est pas obligatoire, nous vous recommandons d'activer le [chiffrement côté serveur](#) pour les compartiments S3 dans lesquels vous stockez les AMI.

Pour plus d'informations sur la définition des paramètres de sécurité appropriés pour vos compartiments S3, consultez les rubriques de sécurité suivantes :

- [Blocage de l'accès public à votre stockage Amazon S3](#)
- [Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3](#)
- [Quelle politique de compartiment S3 puis-je utiliser pour me conformer à la AWS Config règle s3-bucket-ssl-requests-only ?](#)
- [Activation de la journalisation des accès au serveur Amazon S3](#)

Lorsque les instantanés de l'AMI sont copiés vers l'objet S3, la copie des données s'effectue via des connexions TLS. Vous pouvez stocker des AMI avec des instantanés chiffrés, mais les instantanés sont déchiffrés dans le cadre du processus de stockage.

Autorisations de stockage et de restauration des AMI à l'aide de S3

Si vos principaux IAM stockent ou restaurent des AMI à l'aide d'Amazon S3, vous devez leur accorder les autorisations requises.

L'exemple de politique suivant inclut toutes les actions requises pour permettre à un principal IAM d'exécuter les tâches de stockage et de restauration.

Vous pouvez également créer des politiques IAM qui accordent aux principaux l'accès à des ressources spécifiques uniquement. Pour d'autres exemples de politiques, consultez la section [Gestion de l'accès aux AWS ressources](#) dans le Guide de l'utilisateur IAM.

Note

Si les instantanés qui composent l'AMI sont chiffrés ou si votre compte est activé pour le chiffrement par défaut, votre principal IAM doit être autorisé à utiliser la clé KMS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:AbortMultipartUpload",
        "ebs:CompleteSnapshot",
        "ebs:GetSnapshotBlock",
        "ebs:ListChangedBlocks",
        "ebs:ListSnapshotBlocks",
        "ebs:PutSnapshotBlock",
        "ebs:StartSnapshot",
        "ec2:CreateStoreImageTask",
```

```
        "ec2:DescribeStoreImageTasks",
        "ec2:CreateRestoreImageTask",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeTags",
        "ec2:CreateTags"
    ],
    "Resource": "*"
}
]
```

Utilisation des API de stockage et de restauration des AMI

Rubriques

- [Stocker une AMI dans un compartiment S3](#)
- [Décrire la progression d'une tâche de stockage d'AMI](#)
- [Restaurer une AMI à partir d'un compartiment S3](#)

Stocker une AMI dans un compartiment S3

Pour stocker une AMI (AWS CLI)

Utilisez la commande [create-store-image-task](#). Spécifiez l'ID de l'AMI et le nom du compartiment S3 dans lequel stocker l'AMI.

```
aws ec2 create-store-image-task \  
  --image-id ami-1234567890abcdef0 \  
  --bucket myamibucket
```

Sortie attendue

```
{  
  "ObjectKey": "ami-1234567890abcdef0.bin"  
}
```

Décrire la progression d'une tâche de stockage d'AMI

Pour décrire la progression d'une tâche de stockage d'AMI (AWS CLI)

Utilisez la commande [describe-store-image-tasks](#).

```
aws ec2 describe-store-image-tasks
```

Sortie attendue

```
{
  "AmiId": "ami-1234567890abcdef0",
  "Bucket": "myamibucket",
  "ProgressPercentage": 17,
  "S3ObjectKey": "ami-1234567890abcdef0.bin",
  "StoreTaskState": "InProgress",
  "StoreTaskFailureReason": null,
  "TaskStartTime": "2021-01-01T01:01:01.001Z"
}
```

Restaurer une AMI à partir d'un compartiment S3

Pour restaurer une AMI (AWS CLI)

Utilisez la commande [create-restore-image-task](#). À l'aide des valeurs de `S3ObjectKey` et `Bucket` à partir du résultat `describe-store-image-tasks`, spécifiez la clé d'objet de l'AMI et le nom du compartiment S3 dans lequel l'AMI a été copiée. Spécifiez également un nom pour l'AMI restaurée. Le nom doit être unique pour les AMI de la région pour ce compte.

Note

L'AMI restaurée obtient un nouvel ID d'AMI.

```
aws ec2 create-restore-image-task \
  --object-key ami-1234567890abcdef0.bin \
  --bucket myamibucket \
  --name "New AMI Name"
```

Sortie attendue

```
{
  "ImageId": "ami-0eab20fe36f83e1a8"
}
```

Utilisation de chemins d'accès aux fichiers dans S3

Vous pouvez utiliser des chemins d'accès aux fichiers lors du stockage et de la restauration des AMI, de la manière suivante :

- Lorsque vous stockez une AMI dans S3, le chemin d'accès au fichier peut être ajouté au nom du compartiment. En interne, le système sépare le chemin d'accès du nom du compartiment, puis ajoute le chemin d'accès à la clé d'objet générée pour stocker l'AMI. Le chemin d'accès complet à l'objet est indiqué dans la réponse à l'appel d'API.
- Lors de la restauration de l'AMI, étant donné qu'un paramètre de clé d'objet est disponible, le chemin d'accès peut être ajouté au début de la valeur clé de l'objet.

Vous pouvez utiliser des chemins de fichiers lorsque vous utilisez les SDK AWS CLI et.

Exemple : utilisation d'un chemin de fichier lors du stockage et de la restauration d'une AMI (AWS CLI)

L'exemple suivant stocke d'abord une AMI dans S3, avec le chemin d'accès au fichier ajouté au nom du compartiment. L'exemple restaure ensuite l'AMI à partir de S3, avec le chemin d'accès au fichier ajouté au paramètre de clé d'objet.

1. Stockez l'AMI. Pour `--bucket`, indiquez le chemin d'accès au fichier après le nom du compartiment, comme suit :

```
aws ec2 create-store-image-task \  
  --image-id ami-1234567890abcdef0 \  
  --bucket myamibucket/path1/path2
```

Sortie attendue

```
{  
  "ObjectKey": "path1/path2/ami-1234567890abcdef0.bin"  
}
```

2. Restaurez l'AMI. Pour `--object-key`, indiquez la valeur de la sortie de l'étape précédente, qui inclut le chemin d'accès au fichier.

```
aws ec2 create-restore-image-task \  
  --object-key path1/path2/ami-1234567890abcdef0.bin \  
  --image-id ami-1234567890abcdef0
```

```
--bucket myamibucket \  
--name "New AMI Name"
```

Rendre obsolète une AMI

Vous pouvez rendre obsolète une AMI pour indiquer qu'elle ne doit pas être utilisée. Vous pouvez également spécifier une date d'obsolescence future pour une AMI, indiquant quand elle ne devra plus être utilisée. Par exemple, vous pouvez rendre obsolète une AMI qui ne fait plus l'objet d'une maintenance active, ou qui a été remplacée par une version plus récente. Par défaut, les AMI obsolètes n'apparaissent pas dans les listes d'AMI, ce qui empêche les nouveaux utilisateurs d'utiliser out-of-date les AMI. Toutefois, des utilisateurs existants et des services de lancement, tels que des modèles de lancement et des groupes Auto Scaling, peuvent continuer à utiliser une AMI obsolète en spécifiant son ID. Pour supprimer l'AMI afin que les utilisateurs et les services ne puissent plus l'utiliser, vous devez la [désinscrire](#).

Une fois qu'une AMI est obsolète :

- Pour les utilisateurs d'AMI, l'AMI obsolète n'apparaît pas dans les appels d'[DescribeImagesAPI](#), sauf si vous spécifiez son ID ou si vous spécifiez que les AMI obsolètes doivent apparaître. Les propriétaires d'AMI continuent de voir des AMI obsolètes dans les appels d'[DescribeImagesAPI](#).
- Pour les utilisateurs de l'AMI, celle-ci n'est pas disponible pour sélection via la console EC2. Par exemple, une AMI obsolète n'apparaît pas dans le catalogue des AMI dans l'assistant d'instance de lancement. Les propriétaires de l'AMI continuent de voir celle-ci dans la console EC2.
- Pour les utilisateurs de l'AMI, s'ils connaissent son ID, ils peuvent continuer l'utiliser pour lancer des instances à l'aide de l'API, de la CLI ou des kits SDK.
- Des services de lancement tels que des modèles de lancement et des groupes Auto Scaling peuvent continuer à référencer des AMI obsolètes.
- Les instances EC2 lancées à l'aide d'une AMI qui devient obsolète par la suite ne sont pas affectées, et peuvent être arrêtées, démarrées et redémarrées.

Vous pouvez rendre obsolètes des AMI privées et publiques.

Vous pouvez également créer des politiques d'AMI basées sur Amazon Data Lifecycle Manager pour automatiser l'obsolescence des AMI EBS. Pour plus d'informations, consultez [Automatiser les cycles de vie des AMI](#).

Note

Par défaut, la date d'obsolescence de toutes les AMI publiques est fixée à deux ans à compter de la date de création de l'AMI. Vous pouvez définir la date d'obsolescence à moins de deux ans. Pour annuler la date d'obsolescence ou pour la repousser, vous devez rendre l'AMI privée en [la partageant avec des comptes AWS spécifiques](#) uniquement.

Rubriques

- [Coûts](#)
- [Limites](#)
- [Rendre obsolète une AMI](#)
- [Décrire des AMI obsolètes](#)
- [Annuler l'obsolescence d'une AMI](#)

Coûts

Lorsque vous rendez obsolète une AMI, celle-ci n'est pas supprimée. Le propriétaire de l'AMI continue de payer pour les instantanés de celle-ci. Pour arrêter de payer pour les instantanés, le propriétaire de l'AMI doit supprimer celle-ci en la [désinscrivant](#).

Limites

- Pour rendre obsolète une AMI, vous devez en être le propriétaire.

Rendre obsolète une AMI

Vous pouvez rendre obsolète une AMI à une date et une heure spécifiques. Pour ce faire, vous devez être le propriétaire de l'AMI.

Console

Pour rendre obsolète une AMI à une date spécifique ()

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le navigateur de gauche, choisissez AMIs (AMI).

3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).
4. Sélectionnez l'AMI, puis choisissez Actions, Manage AMI Deprecation (Gérer l'obsolescence de l'AMI). Vous pouvez sélectionner plusieurs AMI pour définir la même date d'obsolescence.
5. Cochez la case Enable (Activer), puis saisissez la date et l'heure d'obsolescence.

La limite supérieure de la date d'obsolescence est fixée à 10 ans à partir de maintenant, sauf pour les AMI publiques, où la limite supérieure est de 2 ans à compter de la date de création. Vous ne pouvez pas spécifier de date antérieure.

6. Choisissez Enregistrer.

AWS CLI

Pour rendre obsolète une AMI à une date spécifique ()

Utilisez la commande [enable-image-deprecation](#). Spécifiez l'ID de l'AMI, ainsi que la date et l'heure auxquelles la rendre obsolète. Si vous spécifiez une valeur pour les secondes, Amazon EC2 arrondit les secondes à la minute la plus proche.

La limite supérieure de `deprecate-at` est fixée à 10 ans à partir de maintenant, sauf pour les AMI publiques, où la limite supérieure est de 2 ans à compter de la date de création. Vous ne pouvez pas spécifier de date antérieure.

```
aws ec2 enable-image-deprecation \  
  --image-id ami-1234567890abcdef0 \  
  --deprecate-at "2021-10-15T13:17:12.000Z"
```

Sortie attendue

```
{  
  "Return": "true"  
}
```

Vérifiez quand une AMI a été utilisée pour la dernière fois

`LastLaunchedTime` est un horodatage qui indique quand votre AMI a été utilisée pour la dernière fois pour lancer une instance. Les AMI qui n'ont pas été utilisées récemment pour le démarrage d'une instance peuvent être dépréciées ou [désenregistrés](#).

Note

- Lorsque l'AMI est utilisée pour le démarrage d'une instance, un délai de 24 heures s'écoule avant que cette utilisation ne soit signalée.
- `lastLaunchedTime` les données sont disponibles à partir d'avril 2017.

Console

Pour afficher la dernière heure de lancement d'une AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le navigateur de gauche, choisissez AMIs (AMI).
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).
4. Sélectionnez l'AMI, et ensuite vérifiez le champ Last launched time (Heure du dernier lancement) (si vous avez coché la case à côté de l'AMI, il se situe sur l'onglet Details (Détails)). Le champ affiche la date et l'heure de la dernière utilisation de l'AMI pour le lancement d'une instance.

AWS CLI

Pour afficher la dernière heure de lancement d'une AMI

Exécutez la commande [describe-image-attribute](#) et spécifiez `--attribute lastLaunchedTime`. Pour ce faire, vous devez être le propriétaire de l'AMI.

```
aws ec2 describe-image-attribute \  
  --image-id ami-1234567890example \  
  --attribute lastLaunchedTime
```

Exemple de sortie

```
{  
  "LastLaunchedTime": {  
    "Value": "2022-02-10T02:03:18Z"  
  },  
  "ImageId": "ami-1234567890example",  
}
```

Décrire des AMI obsolètes

Vous pouvez afficher la date et l'heure d'obsolescence d'une AMI et filtrer toutes les AMI par date d'obsolescence. Vous pouvez également utiliser le AWS CLI pour décrire toutes les AMI qui ont été déconseillées, dont la date d'obsolescence remonte au passé.

Console

Pour afficher la date d'obsolescence d'une AMI (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le navigateur de gauche, choisissez AMIs (AMI), puis sélectionnez l'AMI.
3. Vérifiez le champ Deprecation time (Date d'obsolescence) (si vous avez coché la case à côté de l'AMI, il se situe sur l'onglet Details (Détails)). Le champ affiche la date et l'heure d'obsolescence de l'AMI. Si le champ est vide, l'AMI n'est pas obsolète.

Pour filtrer les AMI par date d'obsolescence (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le navigateur de gauche, choisissez AMIs (AMI).
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant) ou Private images (Images privées) (les images privées comprennent les AMI que vous possédez ainsi que celles partagées avec vous).
4. Dans la barre de recherche, saisissez **Deprecation time** (lorsque vous saisissez les lettres, le filtre Deprecation time (Heure d'obsolescence) apparaît), puis choisissez un opérateur, une date et une heure.

AWS CLI

Lorsque vous décrivez toutes les AMI à l'aide de la commande [describe-images](#), les résultats diffèrent selon que vous êtes un utilisateur ou le propriétaire d'une AMI.

- Si vous êtes un utilisateur de l'AMI :

Par défaut, lorsque vous décrivez toutes les AMI à l'aide de la commande [describe-images](#), les AMI obsolètes qui ne vous appartiennent pas mais qui sont partagées avec vous n'apparaissent pas dans les résultats. Cela est dû au fait que la valeur par défaut est `--no-include-`

deprecated. Pour inclure les AMI obsolètes dans les résultats, vous devez spécifier le paramètre `--include-deprecated`.

- Si vous êtes le propriétaire de l'AMI :

Lorsque vous décrivez toutes les AMI à l'aide de la commande [describe-images](#), toutes les AMI dont vous êtes propriétaire, y compris les AMI obsolètes, apparaissent dans les résultats. Vous n'avez pas besoin de spécifier le paramètre `--include-deprecated`. En outre, vous ne pouvez pas exclure des AMI obsolètes dont vous êtes propriétaire à l'aide de la commande `--no-include-deprecated`.

Si une AMI est obsolète, le champ `DeprecationTime` apparaît dans les résultats.

 Note

Une AMI obsolète est une AMI dont la date d'obsolescence est passée. Si vous avez défini la date d'obsolescence sur une date future, l'AMI n'est pas encore obsolète.

Pour inclure toutes les AMI obsolètes lors de la description de toutes les AMI ()

Utilisez la commande [describe-images](#) et spécifiez le paramètre `--include-deprecated` pour inclure dans les résultats toutes les AMI obsolètes dont vous n'êtes pas propriétaire.

```
aws ec2 describe-images \  
  --region us-east-1 \  
  --owners 123456example \  
  --include-deprecated
```

Pour décrire la date d'obsolescence d'une AMI ()

Utilisez la commande [describe-images](#) en spécifiant l'ID de l'AMI.

Notez que si vous spécifiez la commande `--no-include-deprecated` avec l'ID AMI, l'AMI obsolète sera retournée dans les résultats.

```
aws ec2 describe-images \  
  --region us-east-1 \  
  --image-ids ami-1234567890EXAMPLE
```

Sortie attendue

Le champ `DeprecationTime` affiche la date à laquelle l'AMI est définie pour devenir obsolète. Si l'AMI n'est pas définie pour devenir obsolète, le champ `DeprecationTime` n'apparaît pas dans la sortie.

```
{
  "Images": [
    {
      "VirtualizationType": "hvm",
      "Description": "Provided by Red Hat, Inc.",
      "PlatformDetails": "Red Hat Enterprise Linux",
      "EnaSupport": true,
      "Hypervisor": "xen",
      "State": "available",
      "SriovNetSupport": "simple",
      "ImageId": "ami-1234567890EXAMPLE",
      "DeprecationTime": "2021-05-10T13:17:12.000Z",
      "UsageOperation": "RunInstances:0010",
      "BlockDeviceMappings": [
        {
          "DeviceName": "/dev/sda1",
          "Ebs": {
            "SnapshotId": "snap-111222333444aaabb",
            "DeleteOnTermination": true,
            "VolumeType": "gp2",
            "VolumeSize": 10,
            "Encrypted": false
          }
        }
      ],
      "Architecture": "x86_64",
      "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
      "RootDeviceType": "ebs",
      "OwnerId": "123456789012",
      "RootDeviceName": "/dev/sda1",
      "CreationDate": "2019-05-10T13:17:12.000Z",
      "Public": true,
      "ImageType": "machine",
      "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
    }
  ]
}
```

```
}
```

Annuler l'obsolescence d'une AMI

Vous pouvez annuler l'obsolescence d'une AMI, ce qui a pour effet de supprimer la date et l'heure du champ `Deprecation time` (Heure d'obsolescence) (console) ou le champ `DeprecationTime` de la sortie [describe-images](#) (AWS CLI). Pour ce faire, vous devez être le propriétaire de l'AMI.

Console

Pour annuler l'obsolescence d'une AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le navigateur de gauche, choisissez AMIs (AMI).
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).
4. Sélectionnez l'AMI, puis choisissez Actions, Manage AMI Deprecation (Gérer l'obsolescence de l'AMI). Vous pouvez sélectionner plusieurs AMI pour annuler leur dépréciation en même temps.
5. Décochez la case Enable (Activer), puis choisissez Save (Enregistrer).

AWS CLI

Pour annuler l'obsolescence d'une AMI

Utilisez la commande [disable-image-depreciation](#) en spécifiant l'ID de l'AMI.

```
aws ec2 disable-image-deprecation \  
  --image-id ami-1234567890abcdef0
```

Sortie attendue

```
{  
  "Return": "true"  
}
```

Désactiver une AMI

Vous pouvez désactiver une AMI pour empêcher son utilisation pour le lancement d'instances. Vous ne pouvez pas lancer de nouvelles instances à partir d'une AMI désactivée. Vous pouvez réactiver une AMI désactivée afin qu'elle puisse être réutilisée pour le lancement d'instances.

Warning

La désactivation d'une AMI supprime toutes ses autorisations de lancement.

Lorsqu'une AMI est désactivée :

- L'état de l'AMI passe à `disabled`.
- Une AMI désactivée ne peut pas être partagée. Si une AMI était publique ou précédemment partagée, elle devient privée. Si une AMI a été partagée avec une Compte AWS organisation ou une unité organisationnelle, celle-ci perd l'accès à l'AMI désactivée.
- Par défaut, une AMI désactivée n'apparaît pas dans les appels d'API [DescribeImages](#).
- Une AMI désactivée n'apparaît pas dans le filtre de la console M'appartenant. Pour rechercher les AMI désactivées, utilisez le filtre de console Images désactivées.
- Une AMI désactivée ne peut pas être sélectionnée pour le lancement d'une instance dans la console EC2. Par exemple, une AMI désactivée n'apparaît pas dans le catalogue d'AMI dans l'assistant de lancement d'instance ou lors de la création d'un modèle de lancement.
- Des services de lancement tels que des modèles de lancement et des groupes Auto Scaling peuvent continuer à référencer des AMI désactivées. Les lancements d'instance suivants à partir d'une AMI désactivée échoueront. Nous vous recommandons donc de mettre à jour les modèles de lancement et les groupes Auto Scaling afin de ne référencer que les AMI disponibles.
- Les instances EC2 lancées précédemment à l'aide d'une AMI désactivée par la suite ne sont pas affectées et peuvent être arrêtées, démarrées et redémarrées.
- Vous ne pouvez pas supprimer les instantanés associés aux AMI désactivées. Toute tentative de suppression d'un instantané associé entraîne l'erreur `snapshot is currently in use`.

Lorsqu'une AMI est réactivée :

- L'état de l'AMI passe à `available`, et elle peut être utilisée pour lancer des instances.

- L'AMI peut être partagée.
- Les Comptes AWS, les organisations et les unités organisationnelles qui ont perdu l'accès à l'AMI lorsqu'elle a été désactivée n'y ont pas accès à nouveau automatiquement, mais l'AMI peut à nouveau être partagée avec eux.

Vous pouvez désactiver les AMI privées et publiques.

Rubriques

- [Coûts](#)
- [Prérequis](#)
- [Autorisations IAM requises](#)
- [Désactiver une AMI](#)
- [Décrire les AMI désactivées](#)
- [Réactiver une AMI désactivée](#)

Coûts

Lorsque vous désactivez une AMI, celle-ci n'est pas supprimée. Si l'AMI est une AMI basée sur EBS, vous continuez à payer pour les instantanés EBS de l'AMI. Si vous souhaitez conserver l'AMI, vous pouvez peut-être réduire vos coûts de stockage en archivant les instantanés. Pour plus d'informations, consultez la section [Archiver les instantanés Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS. Si vous ne souhaitez pas conserver l'AMI et ses instantanés, vous devez annuler l'enregistrement de l'AMI et supprimer les instantanés. Pour plus d'informations, consultez [Supprimer les ressources associées à votre AMI basée sur Amazon EBS](#).

Prérequis

Pour désactiver ou réactiver une AMI, vous devez en être le propriétaire.

Autorisations IAM requises

Pour désactiver et réactiver une AMI, vous devez disposer des autorisations IAM suivantes :

- `ec2:DisableImage`
- `ec2:EnableImage`

Désactiver une AMI

Vous pouvez désactiver une AMI à l'aide de la console EC2 ou du AWS Command Line Interface (AWS CLI). Pour ce faire, vous devez être le propriétaire de l'AMI.

Console

Pour désactiver une AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation de gauche, choisissez AMI.
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).
4. Sélectionnez l'AMI, puis choisissez Actions, Désactiver l'AMI. Vous pouvez sélectionner plusieurs AMI à désactiver à la fois.
5. Dans la fenêtre Désactiver l'AMI, choisissez Désactiver l'AMI.

AWS CLI

Pour désactiver une AMI

Utilisez la commande [disable-image](#) et spécifiez l'ID de l'AMI.

```
aws ec2 disable-image --image-id ami-1234567890abcdef0
```

Sortie attendue

```
{  
  "Return": "true"  
}
```

Décrire les AMI désactivées

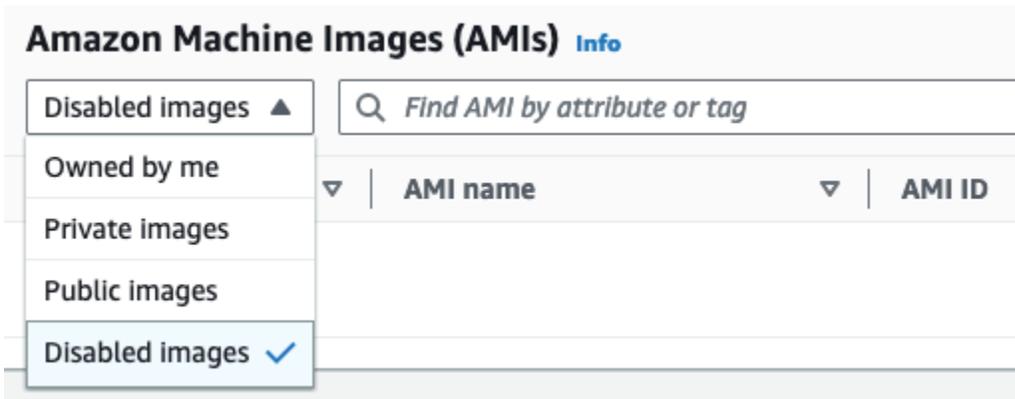
Vous pouvez désactiver une AMI à l'aide de la console EC2 ou de l' AWS CLI.

Vous devez être le propriétaire des AMI pour voir les AMI désactivées. Les AMI désactivées devenant privées, vous ne pouvez pas afficher les AMI désactivées si vous n'en êtes pas le propriétaire.

Console

Pour afficher les AMI désactivées

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation de gauche, choisissez AMI.
3. Dans la barre de filtre, choisissez Images désactivées.



AWS CLI

Par défaut, lorsque vous utilisez la commande [describe-images](#) pour décrire toutes les AMI, les AMI désactivées n'apparaissent pas dans les résultats. Cela est dû au fait que la valeur par défaut est `--no-include-disabled`. Pour inclure les AMI désactivées dans les résultats, vous devez spécifier le paramètre `--include-disabled`.

Pour inclure toutes les AMI désactivées lors de la description de toutes les AMI

Utilisez la commande [describe-images](#) et spécifiez le paramètre `--include-disabled` pour récupérer les AMI désactivées en plus de toutes les autres AMI. Vous pouvez éventuellement spécifier `--owners self` pour ne récupérer que les AMI que vous possédez.

```
aws ec2 describe-images \  
  --region us-east-1 \  
  --owners self \  
  --include-disabled
```

Si vous spécifiez l'ID d'une AMI désactivée, mais que vous ne spécifiez pas `--include-disabled`, l'AMI désactivée est renvoyée dans les résultats.

```
aws ec2 describe-images \  
  --include-disabled
```

```
--region us-east-1 \  
--image-ids ami-1234567890EXAMPLE
```

Pour ne récupérer que les AMI désactivées

Spécifiez `--filters Name=state,Values=disabled`. Vous devez également spécifier `--include-disabled`, sinon vous obtiendrez une erreur.

```
aws ec2 describe-images \  
--include-disabled \  
--filters Name=state,Values=disabled
```

Exemple de sortie

Le champ `State` affiche l'état d'une AMI. `disabled` indique que l'AMI est désactivée.

```
{  
  "Images": [  
    {  
      "VirtualizationType": "hvm",  
      "Description": "Provided by Red Hat, Inc.",  
      "PlatformDetails": "Red Hat Enterprise Linux",  
      "EnaSupport": true,  
      "Hypervisor": "xen",  
      "State": "disabled",  
      "SriovNetSupport": "simple",  
      "ImageId": "ami-1234567890EXAMPLE",  
      "DeprecationTime": "2023-05-10T13:17:12.000Z",  
      "UsageOperation": "RunInstances:0010",  
      "BlockDeviceMappings": [  
        {  
          "DeviceName": "/dev/sda1",  
          "Ebs": {  
            "SnapshotId": "snap-111222333444aaabb",  
            "DeleteOnTermination": true,  
            "VolumeType": "gp2",  
            "VolumeSize": 10,  
            "Encrypted": false  
          }  
        }  
      ],  
      "Architecture": "x86_64",
```

```
    "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
    "RootDeviceType": "ebs",
    "OwnerId": "123456789012",
    "RootDeviceName": "/dev/sda1",
    "CreationDate": "2019-05-10T13:17:12.000Z",
    "Public": false,
    "ImageType": "machine",
    "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
  }
]
}
```

Réactiver une AMI désactivée

Vous pouvez réactiver une AMI désactivée. Pour ce faire, vous devez être le propriétaire de l'AMI.

Console

Pour réactiver une AMI désactivée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation de gauche, choisissez AMI.
3. Dans la barre de filtre, choisissez Images désactivées.
4. Sélectionnez l'AMI, puis choisissez Actions, Activer l'AMI. Vous pouvez sélectionner plusieurs AMI pour en réactiver plusieurs à la fois.
5. Dans la fenêtre Activer l'AMI, sélectionnez Activer.

AWS CLI

Pour réactiver une AMI désactivée

Utilisez la commande [enable-image](#) et spécifiez l'ID de l'AMI.

```
aws ec2 enable-image --image-id ami-1234567890abcdef0
```

Sortie attendue

```
{
```

```
"Return": "true"  
}
```

Archiver des instantanés d'AMI

Vous pouvez archiver les instantanés associés à vos AMI d'EBS désactivées. Cela peut vous aider à réduire les coûts de stockage associés aux AMI que vous utilisez rarement et qui doivent être conservés pendant de longues périodes. Pour plus d'informations, consultez la section [Archiver les instantanés Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Pour archiver les instantanés associés à une AMI

1. [Désactivez l'AMI.](#)
2. [Archivez les instantanés.](#)

Vous ne pouvez pas utiliser une AMI lorsqu'elle est désactivée et que les instantanés qui y sont associés sont archivés.

Pour restaurer une AMI désactivée ayant des instantanés archivés en vue de son utilisation

1. [Restaurez les instantanés archivés](#) associés à l'AMI.
2. [Activez l'AMI.](#)

Désenregistrer (supprimer) une AMI

Lorsque vous annulez l'enregistrement d'une AMI, Amazon EC2 la supprime définitivement. Une fois désenregistré, vous ne pouvez pas utiliser l'AMI pour lancer de nouvelles instances. Vous pouvez envisager de désenregistrer une AMI lorsque vous aurez fini de l'utiliser.

[Pour vous protéger contre le désenregistrement accidentel ou malveillant d'une AMI, vous pouvez activer la protection contre le désenregistrement.](#) Si vous annulez accidentellement l'enregistrement d'une AMI basée sur EBS, vous ne pouvez utiliser [la corbeille](#) pour la restaurer que si vous la restaurez dans le délai imparti avant qu'elle ne soit définitivement supprimée.

L'annulation de l'enregistrement d'une AMI n'a aucun effet sur les instances lancées depuis l'AMI. Vous pouvez continuer à utiliser ces instances. L'annulation de l'enregistrement d'une AMI n'a également aucun effet sur les instantanés créés au cours du processus de création de l'AMI. Vous

continuer de devoir payer des frais d'utilisation pour ces instances et des coûts de stockage pour les instantanés. Par conséquent, pour éviter d'encourir des coûts inutiles, nous vous recommandons de mettre fin à toutes les instances et de supprimer les instantanés dont vous n'avez pas besoin. Pour plus d'informations, consultez [Évitez les coûts liés aux ressources inutilisées](#).

Table des matières

- [Considérations](#)
- [Désenregistrer un AMI](#)
- [Vérifiez quand une AMI a été utilisée pour la dernière fois](#)
- [Protéger une AMI contre le désenregistrement](#)
- [Évitez les coûts liés aux ressources inutilisées](#)

Considérations

- Vous ne pouvez pas annuler l'enregistrement d'une AMI qui n'est pas détenue par votre compte.
- Vous ne pouvez pas utiliser Amazon EC2 pour annuler l'enregistrement d'une AMI gérée par le service. AWS Backup Utilisez-le plutôt AWS Backup pour supprimer les points de restauration correspondants dans le coffre de sauvegarde. Pour plus d'informations, consultez [Suppression des sauvegardes](#) dans le Guide du développeur AWS Backup .

Désenregistrer un AMI

Utilisez l'une des méthodes suivantes pour annuler l'enregistrement d'une AMI basée sur EBS ou d'une AMI basée sur une instance store-backed.

Tip

Pour éviter d'encourir des coûts inutiles, vous devez supprimer toutes les ressources dont vous n'avez pas besoin. Par exemple, pour les AMI basées sur EBS, si vous n'avez pas besoin des instantanés associés à l'AMI désenregistrée, vous devez les supprimer. Pour plus d'informations, consultez [Évitez les coûts liés aux ressources inutilisées](#).

Console

Pour annuler l'enregistrement d'un AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Dans la barre de filtre, choisissez Owned by me pour répertorier vos AMI disponibles, ou choisissez Images désactivées pour répertorier vos AMI désactivées.
4. Sélectionnez l'AMI pour annuler l'enregistrement.
5. Choisissez Actions, Deregister AMI (Annuler l'enregistrement de l'AMI).
6. Lorsque vous êtes invité à confirmer, choisissez Désenregistrer l'AMI.

Plusieurs minutes peuvent être nécessaires pour que la console supprime l'AMI de la liste. Choisissez Refresh pour actualiser le statut.

AWS CLI

Pour annuler l'enregistrement d'un AMI

Utilisez la commande [deregister-image](#) et spécifiez l'ID de l'AMI à désenregistrer.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

Powershell

Pour annuler l'enregistrement d'un AMI

Utilisez l'[Unregister-EC2Image](#) applet de commande et spécifiez l'ID de l'AMI à désenregistrer.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

Vérifiez quand une AMI a été utilisée pour la dernière fois

LastLaunchedTime est un horodatage qui indique quand votre AMI a été utilisée pour la dernière fois pour lancer une instance. Les AMI qui n'ont pas été utilisées récemment pour le démarrage d'une instance peuvent être désenregistrés ou [dépréciées](#).

Note

- Lorsque l'AMI est utilisée pour le démarrage d'une instance, un délai de 24 heures s'écoule avant que cette utilisation ne soit signalée.
- `LastLaunchedTime` les données sont disponibles à partir d'avril 2017.

Console

Pour afficher la dernière heure de lancement d'une AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation de gauche, choisissez AMI.
3. Dans la barre de filtre, choisissez Owned by me (M'appartenant).
4. Sélectionnez l'AMI, et ensuite vérifiez le champ Last launched time (Heure du dernier lancement) (si vous avez coché la case à côté de l'AMI, il se situe sur l'onglet Details (Détails)). Le champ affiche la date et l'heure de la dernière utilisation de l'AMI pour le lancement d'une instance.

AWS CLI

Vous pouvez utiliser la commande [describe-images](#) ou [describe-image-attribute](#) pour afficher l'heure du dernier lancement d'une AMI.

Pour afficher l'heure du dernier lancement d'une AMI à l'aide de `describe-images`

Utilisez la commande [describe-images](#) en spécifiant l'ID de l'AMI.

```
aws ec2 describe-images --image-id ami-0123456789example
```

Exemple de sortie

Note

Le `LastLaunchedTime` champ apparaît uniquement dans la sortie pour les AMI que vous possédez.

```
{
  "Images": [
    {
      ...
      "LastLaunchedTime": {
        "Value": "2024-04-02T02:03:18Z"
      },
      ...
    }
  ]
}
```

Pour afficher la dernière heure de lancement d'une AMI

Utilisez la commande [describe-image-attribute](#) et spécifiez `--attribute lastLaunchedTime`. Vous devez être propriétaire de l'AMI pour exécuter cette commande.

```
aws ec2 describe-image-attribute \
  --image-id ami-0123456789example \
  --attribute lastLaunchedTime
```

Exemple de sortie

```
{
  "ImageId": "ami-1234567890example",
  "LastLaunchedTime": {
    "Value": "2022-02-10T02:03:18Z"
  }
}
```

Protéger une AMI contre le désenregistrement

Vous pouvez activer la protection de désenregistrement sur une AMI pour empêcher toute suppression accidentelle ou malveillante. Lorsque vous activez la protection de désenregistrement, aucun utilisateur ne peut désenregistrer l'AMI, quelles que soient ses autorisations IAM. Si vous souhaitez annuler l'enregistrement de l'AMI, vous devez d'abord désactiver la protection de désenregistrement.

Lorsque vous activez la protection de désenregistrement sur une AMI, vous avez la possibilité d'inclure une période de recharge de 24 heures. Cette période de recharge est la durée pendant

laquelle la protection de désenregistrement reste active une fois que vous l'avez désactivée. Pendant cette période de recharge, l'AMI ne peut pas être désenregistrée. À la fin du délai de recharge, l'AMI peut être désenregistrée.

La protection contre le désenregistrement est désactivée par défaut sur toutes les AMI existantes et nouvelles.

Activer la protection de désenregistrement

Utilisez l'une des méthodes suivantes pour activer la protection de désenregistrement sur une AMI. Pour cela, vous devez être le propriétaire de l'AMI.

Console

Pour activer la protection de désenregistrement sur une AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Dans la barre de filtre, choisissez Owned by me pour répertorier vos AMI disponibles, ou choisissez Images désactivées pour répertorier vos AMI désactivées.
4. Sélectionnez l'AMI sur laquelle vous souhaitez activer la protection de désenregistrement, puis choisissez Actions, Gérer la protection de désenregistrement de l'AMI.
5. Dans la boîte de dialogue Gérer la protection contre le désenregistrement des AMI, vous pouvez activer la protection contre le désenregistrement avec ou sans délai de recharge. Choisissez l'une des options suivantes :
 - Activez avec une période de recharge de 24 heures : avec une période de recharge, l'AMI ne peut pas être désenregistrée pendant 24 heures lorsque la protection contre le désenregistrement est désactivée.
 - Activation sans temps de recharge : sans délai de recharge, l'AMI peut être désenregistrée immédiatement lorsque la protection contre le désenregistrement est désactivée.
6. Choisissez Enregistrer.

AWS CLI

Pour activer la protection de désenregistrement sur une AMI

Utilisez la commande [enable-image-deregistration-protection](#) et spécifiez l'ID de l'AMI. Pour inclure la période de recharge optionnelle de 24 heures, incluez `--with-cooldown set to true`. Pour exclure le délai de recharge, omettez le `--with-cooldown` paramètre.

```
aws ec2 enable-image-deregistration-protection \  
  --image-id ami-0123456789example \  
  --with-cooldown true
```

Désactiver la protection de désenregistrement

Utilisez l'une des méthodes suivantes pour désactiver la protection de désenregistrement sur une AMI. Pour cela, vous devez être le propriétaire de l'AMI.

Note

Si vous avez choisi d'inclure une période de recharge de 24 heures lorsque vous activez la protection de désenregistrement pour l'AMI, vous ne pourrez pas immédiatement annuler l'enregistrement de l'AMI lorsque vous désactiverez la protection de désenregistrement. La période de recharge est la période de 24 heures pendant laquelle la protection de désenregistrement reste en vigueur même après sa désactivation. Pendant cette période de recharge, l'AMI ne peut pas être désenregistrée. Une fois la période de recharge terminée, l'AMI peut être désenregistrée.

Console

Pour désactiver la protection contre le désenregistrement sur une AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Dans la barre de filtre, choisissez Owned by me pour répertorier vos AMI disponibles, ou choisissez Images désactivées pour répertorier vos AMI désactivées.
4. Sélectionnez l'AMI pour désactiver la protection de désenregistrement, puis choisissez Actions, Gérer la protection de désenregistrement de l'AMI.
5. Dans la boîte de dialogue Gérer la protection contre le désenregistrement des AMI, choisissez Désactiver.
6. Choisissez Enregistrer.

AWS CLI

Pour désactiver la protection contre le déenregistrement sur une AMI

Utilisez la commande [disable-image-deregistration-protection](#) et spécifiez l'ID de l'AMI.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0123456789example
```

Évitez les coûts liés aux ressources inutilisées

Lorsque vous désenregistrez une AMI, vous ne supprimez pas les ressources associées à l'AMI. Ces ressources incluent les instantanés des AMI basées sur EBS et les fichiers d'Amazon S3, par exemple les AMI sauvegardées en magasin. Lorsque vous désenregistrez une AMI, vous ne résiliez ni n'arrêtez aucune instance lancée depuis l'AMI.

Vous continuerez à supporter des frais pour le stockage des instantanés et des fichiers, ainsi que pour toutes les instances en cours d'exécution. Pour plus d'informations, consultez [Facturation](#).

Pour éviter ce type de coûts inutiles, nous vous recommandons de supprimer toutes les ressources dont vous n'avez pas besoin.

Pour déterminer si votre AMI est basée sur EBS ou sur un stockage d'instance, consultez [Déterminer le type de périphérique racine de votre AMI](#)

Supprimer les ressources associées à votre AMI basée sur Amazon EBS

Utilisez l'une des méthodes suivantes pour supprimer les ressources associées à votre AMI basée sur EBS.

Console

Pour supprimer les ressources associées à votre AMI basée sur EBS

1. [Désenregistrez l'AMI](#).

Notez l'ID de l'AMI : il peut vous aider à trouver les instantanés à supprimer à l'étape suivante.

2. [Supprimez les instantanés](#) dont vous n'avez pas besoin.

L'ID de l'AMI associée est affiché dans la colonne Description de l'écran Snapshots.

3. [Mettez fin aux instances](#) dont vous n'avez pas besoin.

AWS CLI

Pour supprimer les ressources associées à votre AMI basée sur EBS

1. Désenregistrez l'AMI à l'aide de la commande [deregister-image](#).

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Supprimez les instantanés dont vous n'avez pas besoin à l'aide de la commande [delete-snapshot](#).

```
aws ec2 delete-snapshot --snapshot-id snap-0123456789example
```

3. Mettez fin aux instances dont vous n'avez pas besoin à l'aide de la commande [terminate-instances](#).

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

PowerShell

Pour supprimer les ressources associées à votre AMI basée sur EBS

1. Désenregistrez l'AMI à l'aide de l'applet de [Unregister-EC2Image](#) commande.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

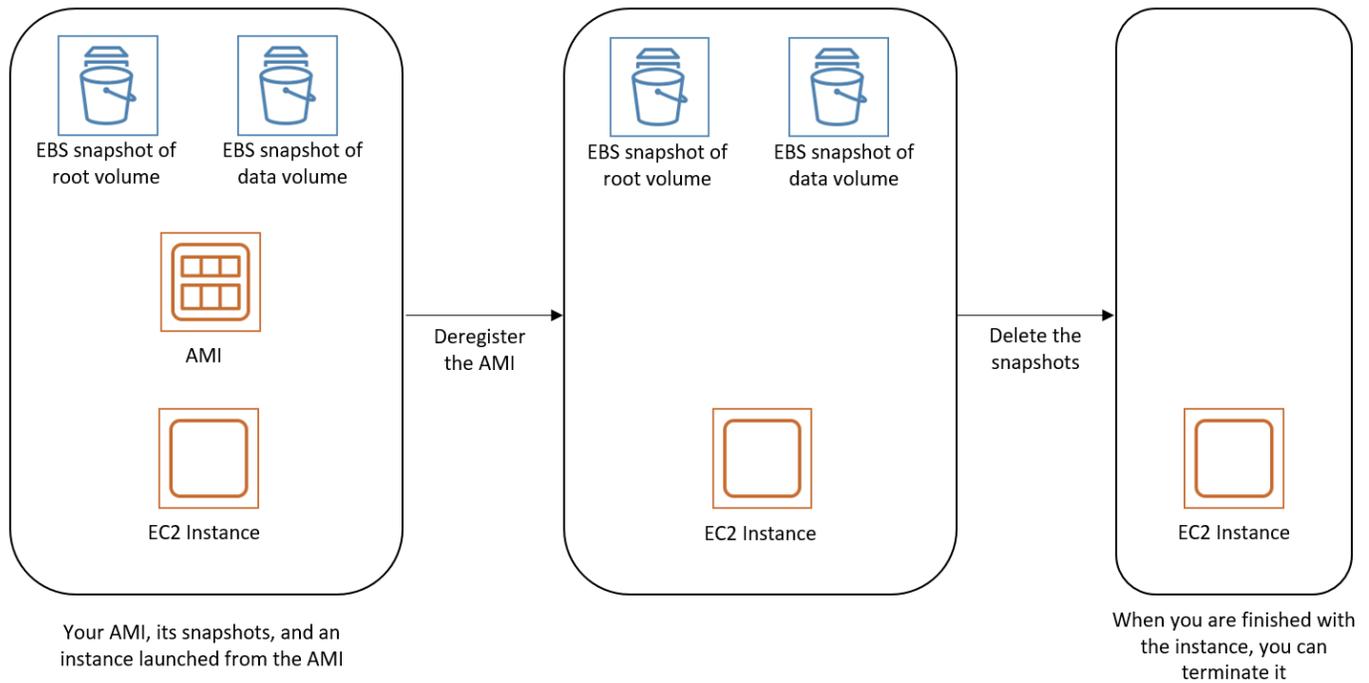
2. Supprimez les instantanés dont vous n'avez pas besoin à l'aide de l'[Remove-EC2Snapshot](#) applet de commande.

```
Remove-EC2Snapshot -SnapshotId snap-0123456789example
```

3. Mettez fin aux instances dont vous n'avez pas besoin à l'aide de l'[Remove-EC2Instance](#) applet de commande.

```
Remove-EC2Instance -InstanceId i-0123456789example
```

Le schéma suivant illustre le flux de suppression des ressources associées à une AMI basée sur EBS.



Supprimer les ressources associées à l'AMI sauvegardée par l'instance store-backed

Utilisez la méthode suivante pour supprimer les ressources associées à votre AMI basée sur une instance store-backed.

Pour supprimer les ressources associées à votre AMI sauvegardée par une instance store-backed

1. Désenregistrez l'AMI à l'aide de la commande [deregister-image](#).

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Supprimez le bundle dans Amazon S3 à l'aide de la commande [ec2-delete-bundle](#) (outils AMI).

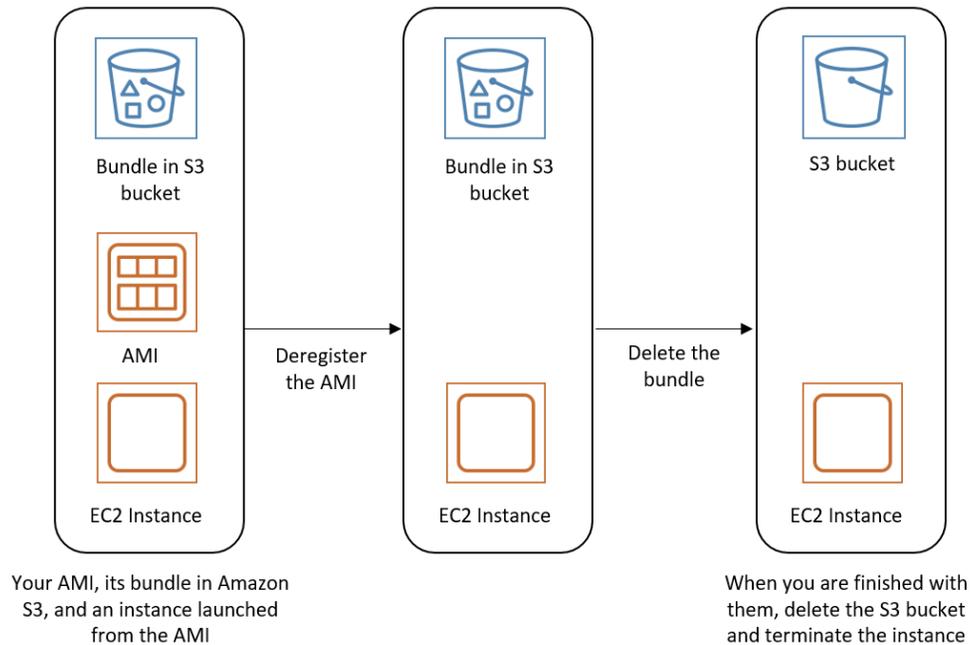
```
ec2-delete-bundle -b myawsbucket/myami -a your_access_key_id -s your_secret_access_key -p image
```

3. Mettez fin aux instances dont vous n'avez pas besoin à l'aide de la commande [terminate-instances](#).

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

4. Si vous en avez terminé avec le compartiment Amazon S3 dans lequel vous avez chargé le bundle, vous pouvez le supprimer. Pour supprimer un compartiment Amazon S3, ouvrez la console Amazon S3, sélectionnez le compartiment, choisissez Actions, puis Delete.

Le schéma suivant illustre le flux de suppression des ressources associées à votre AMI basée sur une instance store-backed.



Automatiser le cycle de vie des AMI basées sur EBS

Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création, la rétention, la copie, l'obsolescence et la suppression des AMI Amazon EBS et de leurs instantanés de sauvegarde. Pour plus d'informations, consultez [Amazon Data Lifecycle Manager](#).

Utiliser le chiffrement avec des AMI basées sur EBS

Les AMI basées sur des instantanés Amazon EBS peuvent tirer parti du chiffrement Amazon EBS. Les instantanés de volumes de données et racine peuvent être chiffrés et attachés à une AMI. Vous pouvez lancer des instances et copier des images avec une prise en charge complète du chiffrement EBS. Les paramètres de chiffrement pour ces opérations sont pris en charge dans toutes les régions où ils AWS KMS sont disponibles.

Les instances EC2 avec des volumes EBS chiffrés sont lancées à partir des AMIs de la même manière que les autres instances. De plus, lorsque vous lancez une instance à partir d'une AMI basée sur des instantanés EBS non chiffrés, vous pouvez chiffrer une partie ou l'ensemble des volumes pendant le lancement.

À l'instar des volumes EBS, les instantanés des AMI peuvent être chiffrés soit par défaut AWS KMS key, soit avec une clé gérée par le client que vous spécifiez. Dans tous les cas, vous devez être autorisé à utiliser la clé KMS sélectionnée.

Les AMI contenant des instantanés chiffrés peuvent être partagées entre AWS comptes. Pour plus d'informations, consultez [AMI partagées](#).

Rubriques relatives au chiffrement avec des AMI basées sur EBS

- [Scénarios de lancement d'instances](#)
- [Scénarios de copie d'images](#)

Scénarios de lancement d'instances

Les instances Amazon EC2 sont lancées à partir d'AMI à l'aide de l'`RunInstances` action avec des paramètres fournis par le biais du mappage de périphériques par blocs, soit au moyen de l'API ou de la CLI Amazon EC2, soit directement à l'aide de l'API AWS Management Console ou de la CLI Amazon EC2. Pour plus d'informations, consultez [Mappages de périphériques de stockage en mode bloc](#). Pour des exemples de contrôle du mappage des périphériques en mode bloc à partir du AWS CLI, voir [Lancer, répertorier et résilier des instances EC2](#).

Par défaut, sans paramètres de chiffrement explicites, une action `RunInstances` conserve l'état de chiffrement existant des instantanés source d'une AMI lors de la restauration des volumes EBS à partir de ceux-ci. Si le chiffrement est activé par défaut, tous les volumes créés à partir de l'AMI (qu'ils soient issus de snapshots chiffrés ou non chiffrés) sont chiffrés. Si le chiffrement par défaut n'est pas activé, l'instance conserve l'état de chiffrement de l'AMI.

Vous pouvez également lancer une instance et, simultanément, appliquer un nouvel état de chiffrement aux volumes créés en spécifiant les paramètres de chiffrement. Dans un tel cas, les comportements suivants sont observés :

Lancement sans paramètres de chiffrement

- Un instantané non chiffré est restauré dans un volume non chiffré, sauf si le chiffrement par défaut est activé, auquel cas tous les volumes nouvellement créés seront chiffrés.
- Un instantané non chiffré que vous possédez est restauré dans un volume qui est chiffré avec la même clé KMS.
- Un instantané chiffré qui ne vous appartient pas (par exemple, l'AMI est partagée avec vous) est restauré sur un volume chiffré par la clé KMS par défaut de votre AWS compte.

Les comportements par défaut peuvent être ignorés en spécifiant les paramètres de chiffrement. Les paramètres disponibles sont `Encrypted` et `KmsKeyId`. La définition du seul paramètre `Encrypted` produit les effets suivants :

Comportements en cas de lancement d'instance avec le paramètre **Encrypted** défini, mais sans spécifier le paramètre **KmsKeyId**

- Un instantané non chiffré est restauré dans un volume EBS qui est chiffré avec la clé KMS par défaut de votre compte AWS .
- Un instantané chiffré que vous possédez est restauré dans un volume EBS qui est chiffré avec la même clé KMS. (En d'autres mots, le paramètre `Encrypted` est sans effet.)
- Un instantané chiffré qui ne vous appartient pas (c'est-à-dire que l'AMI est partagée avec vous) est restauré sur un volume chiffré par la clé KMS par défaut de votre AWS compte. (En d'autres mots, le paramètre `Encrypted` est sans effet.)

La définition des paramètres `Encrypted` et `KmsKeyId` vous permet de spécifier une clé KMS autre que la clé par défaut pour une opération de chiffrement. Les comportements suivants sont observés :

Instance avec définition des paramètres **Encrypted** et **KmsKeyId**

- Un instantané non chiffré est restauré dans un volume EBS qui est chiffré avec la clé KMS spécifiée.
- Un instantané chiffré est restauré dans un volume EBS qui est chiffré non pas avec la clé KMS d'origine mais avec la clé KMS spécifiée.

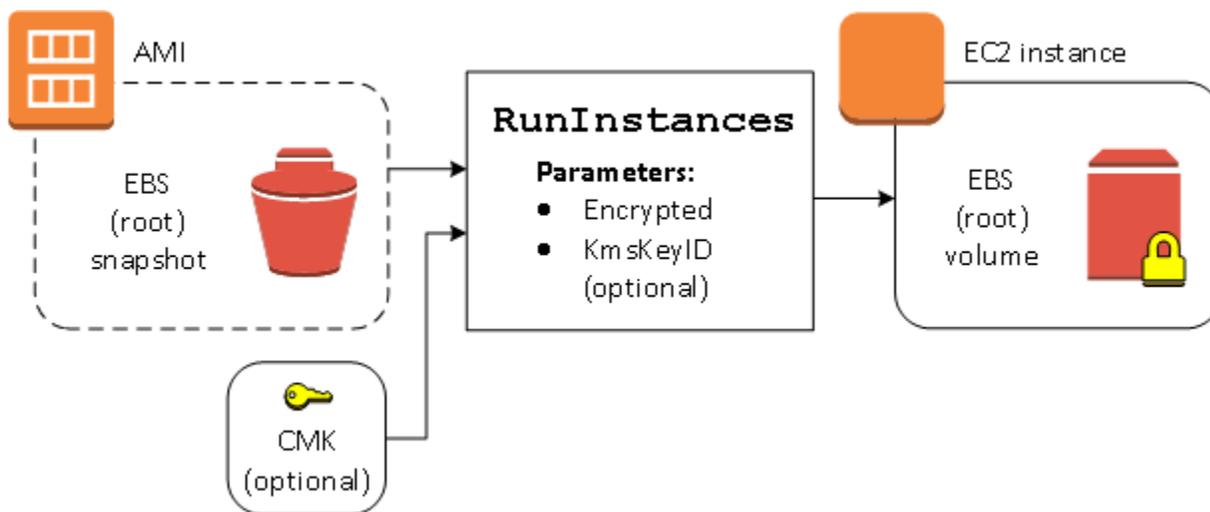
L'envoi de `KmsKeyId` sans définir également le paramètre `Encrypted` génère une erreur.

Les sections suivantes fournissent des exemples de lancement d'instances à partir d'AMI avec des paramètres de chiffrement autres que les paramètres par défaut. Dans chacun de ces scénarios, les paramètres fournis à l'action `RunInstances` entraînent un changement de l'état de chiffrement pendant la restauration d'un volume à partir d'un instantané.

Pour plus d'informations sur l'utilisation de la console pour lancer une instance à partir d'une AMI, consultez la section [Lancer votre instance](#).

Chiffrement d'un volume pendant le lancement

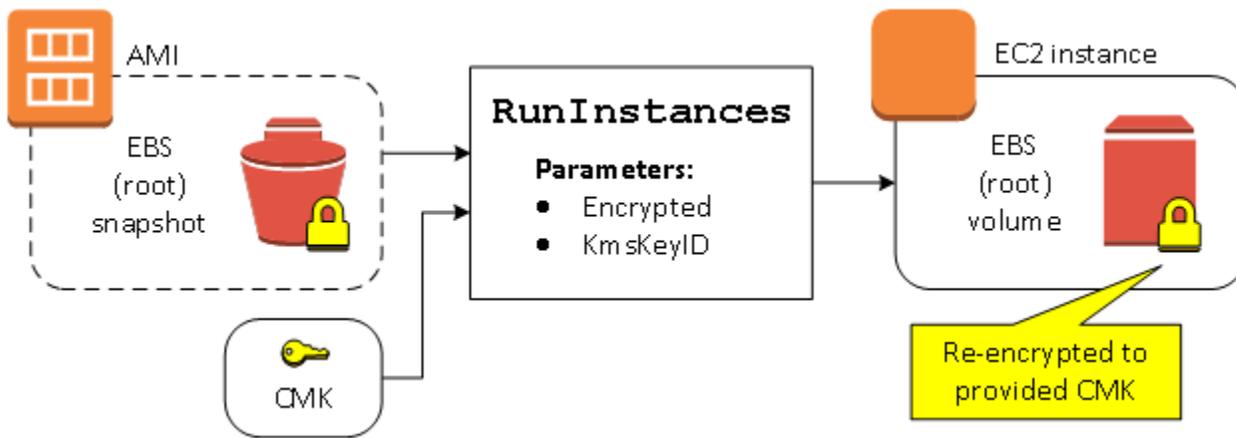
Dans cet exemple, une AMI basée sur un instantané non chiffré est utilisée pour lancer une instance EC2 avec un volume EBS chiffré.



Le paramètre `Encrypted` seul entraîne le chiffrement du volume pour cette instance. Le paramètre `KmsKeyId` est facultatif. Si aucun ID de clé KMS n'est spécifié, la clé KMS par défaut du AWS compte est utilisée pour chiffrer le volume. Pour chiffrer le volume avec une autre clé KMS que vous possédez, fournissez le paramètre `KmsKeyId`.

Rechiffrement d'un volume pendant le lancement

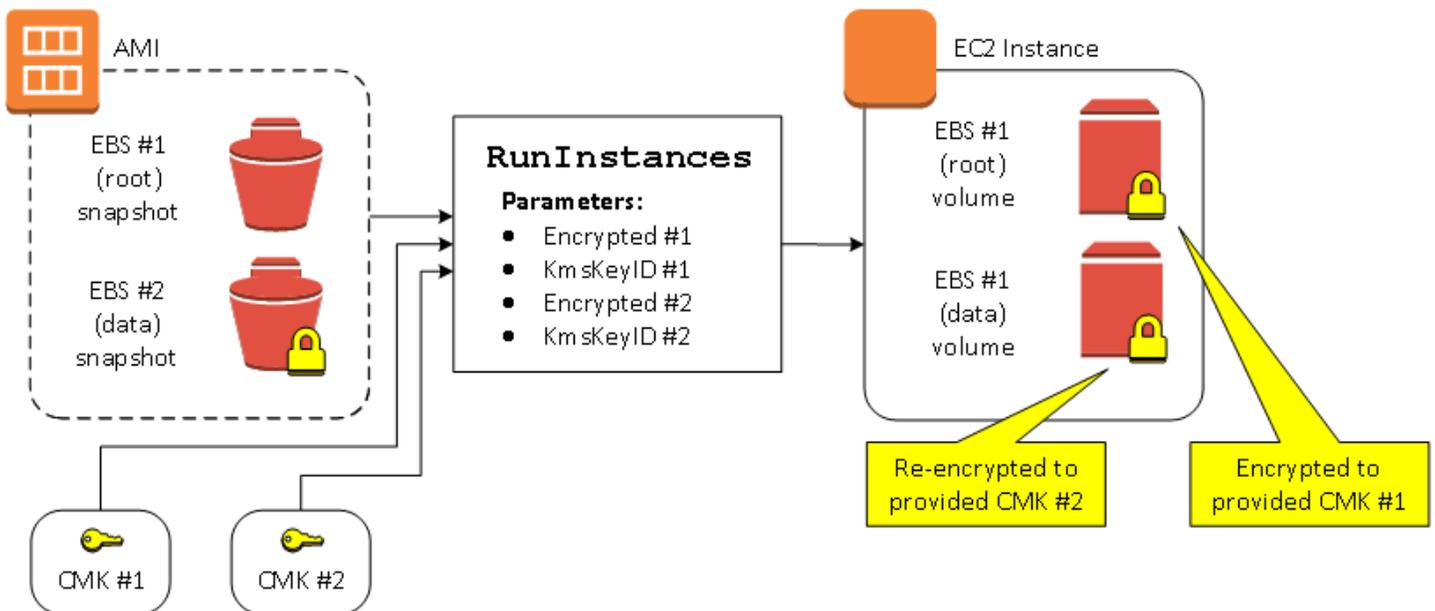
Dans cet exemple, une AMI basée sur un instantané chiffré est utilisée pour lancer une instance EC2 avec un volume EBS chiffré à l'aide d'une nouvelle clé KMS.



Si vous possédez l'AMI et que vous ne spécifiez pas de paramètres de chiffrement, l'instance obtenue dispose d'un volume chiffré avec la même clé KMS que l'instantané. Si l'AMI est partagée avec vous mais que vous n'en êtes pas propriétaire, et si vous ne spécifiez pas de paramètres de chiffrement, le volume est chiffré avec votre clé KMS par défaut. Avec les paramètres de chiffrement fournis, comme illustré, le volume est chiffré avec la clé KMS spécifiée.

Modification de l'état de chiffrement de plusieurs volumes pendant le lancement

Dans cet exemple plus complexe, une AMI basée sur plusieurs instantanés (chacun avec son propre état de chiffrement) est utilisée pour lancer une instance EC2 avec un volume nouvellement chiffré et un volume re-chiffré.



Dans ce scénario, l'action `RunInstances` reçoit des paramètres de chiffrement pour chacun des instantanés source. Lorsque tous les paramètres de chiffrement sont spécifiés, l'instance créée est la même, que vous possédiez ou non l'AMI.

Scénarios de copie d'images

Les AMI Amazon EC2 sont copiées au moyen de l'action `CopyImage`, soit via la AWS Management Console, soit directement avec l'API Amazon EC2 ou la CLI.

Par défaut, sans paramètres de chiffrement explicites, une action `CopyImage` conserve l'état de chiffrement existant des instantanés source d'une AMI lors de la copie. Vous pouvez également copier une AMI et, simultanément, appliquer un nouvel état de chiffrement à ses instantanés EBS associés en spécifiant les paramètres de chiffrement. Dans un tel cas, les comportements suivants sont observés :

Copie sans paramètres de chiffrement

- Un instantané non chiffré est copié dans un autre instantané non chiffré, sauf si le chiffrement par défaut est activé, auquel cas tous les instantanés nouvellement créés seront chiffrés.
- Un instantané chiffré que vous possédez est copié dans un instantané chiffré avec la même clé KMS.
- Un instantané chiffré qui ne vous appartient pas (c'est-à-dire que l'AMI est partagée avec vous) est copié dans un instantané chiffré par la clé KMS par défaut de votre AWS compte.

Tous ces comportements par défaut peuvent être ignorés en spécifiant les paramètres de chiffrement. Les paramètres disponibles sont `Encrypted` et `KmsKeyId`. La définition du seul paramètre `Encrypted` produit les effets suivants :

Comportements en cas de copie-image avec le paramètre **Encrypted** défini, mais pas le paramètre **KmsKeyId**

- Un instantané non chiffré est copié dans un instantané chiffré avec la clé KMS par défaut du compte AWS.
- Un instantané chiffré est copié dans un instantané chiffré avec la même clé KMS. (En d'autres mots, le paramètre `Encrypted` est sans effet.)
- Un instantané chiffré qui ne vous appartient pas (c'est-à-dire que l'AMI est partagée avec vous) est copié sur un volume chiffré à l'aide de la clé KMS par défaut de votre AWS compte. (En d'autres mots, le paramètre `Encrypted` est sans effet.)

La définition des paramètres `Encrypted` et `KmsKeyId` vous permet de spécifier une clé KMS gérée par le client pour une opération de chiffrement. Les comportements suivants sont observés :

Comportements en cas de copie-image avec les paramètres **Encrypted** et **KmsKeyId** définis

- Un instantané non chiffré est copié dans un instantané chiffré avec la clé KMS spécifiée.
- Un instantané chiffré est copié dans un instantané qui est chiffré non pas avec la clé KMS d'origine mais avec la clé KMS spécifiée.

L'envoi de `KmsKeyId` sans définir également le paramètre `Encrypted` génère une erreur.

La section suivante fournit un exemple de copie d'une AMI avec des paramètres de chiffrement personnalisés, ce qui entraîne un changement de l'état de chiffrement.

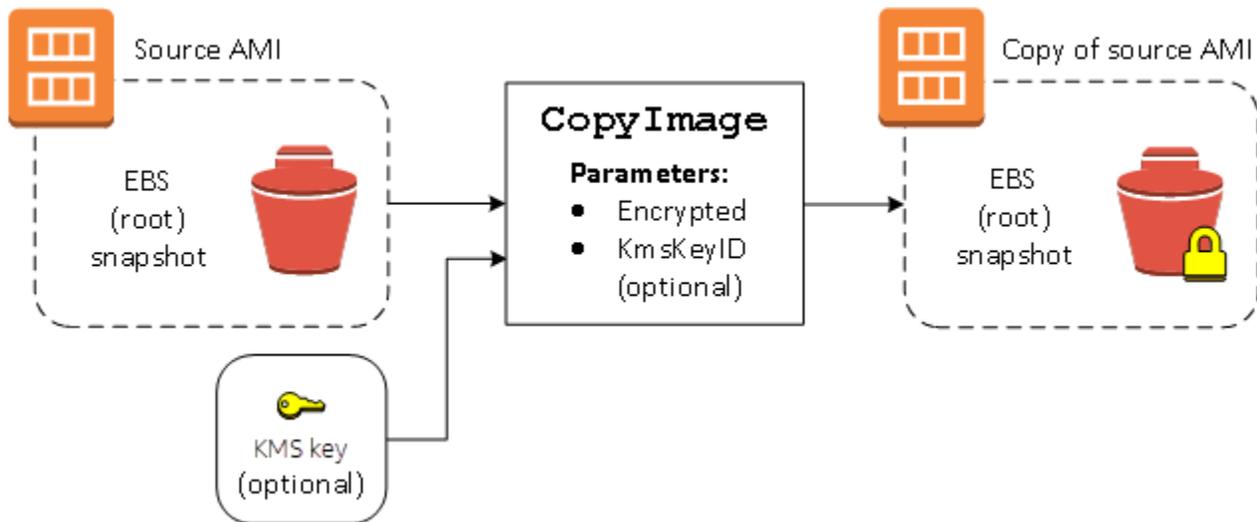
Pour obtenir des instructions détaillées sur l'utilisation de la console, consultez la section [Copier une AMI](#).

Chiffrement d'une image non chiffrée pendant la copie

Dans ce scénario, une AMI basée sur un instantané racine non chiffré est copiée sur une AMI avec un instantané racine chiffré. L'action `CopyImage` est appelée avec deux paramètres de chiffrement, y compris une clé gérée par le client. Par conséquent, l'état de chiffrement de l'instantané racine change, de sorte que l'AMI cible est basée sur un instantané racine contenant les mêmes données que l'instantané source, mais chiffrée à l'aide de la clé spécifiée. Vous supportez des coûts de stockage pour les instantanés dans les deux AMI, ainsi que des frais pour toutes les instances que vous lancez à partir de l'une ou l'autre AMI.

Note

L'activation du chiffrement par défaut a le même effet que la définition du `Encrypted` paramètre sur `true` pour tous les instantanés de l'AMI.



Définir le paramètre `Encrypted` chiffre l'instantané unique de cette instance. Si vous ne spécifiez pas le paramètre `KmsKeyId`, la clé gérée par le client par défaut est utilisée pour chiffrer la copie de l'instantané.

Note

Vous pouvez également copier une image avec plusieurs instantanés et configurer l'état de chiffrement de chacun individuellement.

Surveillez les événements AMI à l'aide d'Amazon EventBridge

Lorsque l'état d'une Amazon Machine Image (AMI) change, Amazon EC2 génère un événement qui est envoyé à Amazon EventBridge (anciennement Amazon CloudWatch Events). Vous pouvez utiliser Amazon EventBridge pour détecter ces événements et y réagir. Pour ce faire, vous devez créer des règles EventBridge qui déclenchent une action en réponse à un événement. Par exemple, vous pouvez créer une EventBridge règle qui détecte la fin du processus de création de l'AMI, puis qui invoque une rubrique Amazon SNS pour vous envoyer une notification par e-mail.

Amazon EC2 génère un événement lorsqu'une AMI entre dans l'un des états suivants :

- `available`
- `failed`
- `deregistered`
- `disabled`

Le tableau suivant répertorie les opérations d'AMI et les états dans lesquels une AMI peut basculer. Dans le tableau, Oui indique les états dans lesquels l'AMI peut basculer lors de l'exécution de l'opération correspondante.

Opérations de l'AMI	available	failed	deregistered	disabled
CopyImage	Oui	Oui		
CreateImage	Oui	Oui		
CreateRes-toreImageTask	Oui	Oui		
DeregisterImage			Oui	
DisableImage				Oui
EnableImage	Oui			
RegisterImage	Oui	Oui		

Les événements sont générés sur la base du meilleur effort.

Rubriques

- [Événements AMI](#)
- [Créez des EventBridge règles Amazon](#)

Événements AMI

Il existe quatre événements EC2 AMI State Change :

- [available](#)
- [failed](#)
- [deregistered](#)
- [disabled](#)

Les événements sont envoyés au bus d' EventBridge événements par défaut au format JSON.

Les champs suivants de l'événement peuvent être utilisés pour créer des règles qui déclenchent une action :

```
"source": "aws.ec2"
```

Identifie que l'événement provient de Amazon EC2.

```
"detail-type": "EC2 AMI State Change"
```

Identifie le nom de l'événement.

```
"detail": { "ImageId": "ami-0123456789example", "State": "available", }
```

Fournit les informations suivantes :

- L'ID de l'AMI : si vous souhaitez suivre une AMI spécifique.
- L'état de l'AMI (available, failed, deregistered ou disabled).

available

Voici un exemple d'événement généré par Amazon EC2 lorsque l'AMI bascule dans l'état available après une opération CreateImage, CopyImage, RegisterImage, CreateRestoreImageTask ou EnableImage réussie.

"State": "available" indique que l'opération a réussi.

```
{
  "version": "0",
  "id": "example-9f07-51db-246b-d8b8441bcd0",
  "detail-type": "EC2 AMI State Change",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
  "detail": {
    "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
    "ImageId": "ami-0123456789example",
    "State": "available",
    "ErrorMessage": ""
  }
}
```

failed

Voici un exemple d'événement généré par Amazon EC2 lorsque l'AMI bascule dans l'état `failed` après l'échec d'une opération `CreateImage`, `CopyImage`, `RegisterImage` ou `CreateRestoreImageTask`.

Les champs suivants fournissent des informations pertinentes :

- `"State": "failed"` : indique que l'opération a échoué.
- `"ErrorMessage": ""` : indique la raison de l'échec de l'opération.

```
{
  "version": "0",
  "id": "example-9f07-51db-246b-d8b8441bcdf0",
  "detail-type": "EC2 AMI State Change",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
  "detail": {
    "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
    "ImageId": "ami-0123456789example",
    "State": "failed",
    "ErrorMessage": "Description of failure"
  }
}
```

deregistered

Voici un exemple d'événement généré par Amazon EC2 lorsque l'AMI bascule dans l'état `deregistered` après une opération `DeregisterImage` réussie. Si l'opération échoue, aucun événement n'est généré. Tout échec est immédiatement connu, car `DeregisterImage` est une opération synchrone.

`"State": "deregistered"` indique que l'opération `DeregisterImage` a réussi.

```
{
  "version": "0",
  "id": "example-9f07-51db-246b-d8b8441bcdf0",
  "detail-type": "EC2 AMI State Change",
```

```

"source": "aws.ec2",
"account": "012345678901",
"time": "yyyy-mm-ddThh:mm:ssZ",
"region": "us-east-1",
"resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
"detail": {
  "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
  "ImageId": "ami-0123456789example",
  "State": "deregistered",
  "ErrorMessage": ""
}
}

```

disabled

Voici un exemple d'événement généré par Amazon EC2 lorsque l'AMI bascule dans l'état `disabled` après une opération `DisableImage` réussie. Si l'opération échoue, aucun événement n'est généré. Tout échec est immédiatement connu, car `DisableImage` est une opération synchrone.

"State": "disabled" indique que l'opération `DisableImage` a réussi.

```

{
  "version": "0",
  "id": "example-9f07-51db-246b-d8b8441bcdf0",
  "detail-type": "EC2 AMI State Change",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
  "detail": {
    "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
    "ImageId": "ami-0123456789example",
    "State": "disabled",
    "ErrorMessage": ""
  }
}

```

Créez des EventBridge règles Amazon

Vous pouvez créer une EventBridge [règle](#) Amazon qui spécifie une action à effectuer lors de la EventBridge réception d'un [événement](#) qui correspond au [modèle d'événement](#) défini dans la règle.

Lorsqu'un événement correspond, EventBridge envoie l'événement à la [cible](#) spécifiée et déclenche l'action définie dans la règle.

Les modèles d'événement ont la même structure que les événements auxquels ils correspondent. Soit un modèle d'événement correspond à un événement, soit il n'y correspond pas.

Lorsque vous créez une règle pour un événement de changement d'état d'AMI, vous pouvez inclure les champs suivants dans le modèle d'événement :

```
"source": "aws.ec2"
```

Identifie que l'événement provient de Amazon EC2.

```
"detail-type": "EC2 AMI State Change"
```

Identifie le nom de l'événement.

```
"detail": { "ImageId": "ami-0123456789example", "State": "available", }
```

Fournit les informations suivantes :

- L'ID de l'AMI : si vous souhaitez suivre une AMI spécifique.
- L'état de l'AMI (available, failed, deregistered ou disabled).

Exemple : créer une EventBridge règle pour envoyer une notification

L'exemple suivant crée une EventBridge règle pour envoyer un e-mail, un message texte ou une notification push mobile lorsqu'une AMI est dans son `available` état une fois l'`CreateImage` opération terminée avec succès.

Avant de créer la EventBridge règle, vous devez créer la rubrique Amazon SNS pour l'e-mail, le message texte ou la notification push mobile.

Pour créer une EventBridge règle permettant d'envoyer une notification lorsqu'une AMI est créée et qu'elle est dans l'**available** état

1. Ouvrez la EventBridge console Amazon à l'[adresse https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Choisissez Créer une règle.
3. Pour Define rule detail (Définir les détails de la règle), procédez comme suit :
 - a. Entrez un nom et éventuellement une description pour la règle.

Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

- b. Pour Event bus (Bus d'événement), choisissez default (défaut). Lorsqu'un service AWS de votre compte génère un événement, il accède toujours au bus d'événement par défaut de votre compte.
 - c. Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
 - d. Choisissez Suivant.
4. Pour Build event pattern (Créer un modèle d'événement), procédez comme suit :
- a. Dans Source de l'événement, sélectionnez AWS événements ou événements EventBridge partenaires.
 - b. Pour Event pattern (Modèle d'événement), pour cet exemple, vous allez spécifier le modèle d'événement suivant pour correspondre à n'importe quel événement EC2 AMI State Change qui est généré lorsqu'une AMI entre dans l'état available :

```
{
  "source": ["aws.ec2"],
  "detail-type": ["EC2 AMI State Change"],
  "detail": {"State": ["available"]}
}
```

Pour ajouter le modèle d'événement, vous pouvez utiliser un modèle en choisissant Event pattern form (Formulaire de modèle d'événement), ou spécifiez votre propre modèle en choisissant Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]), comme suit :

- i. Pour utiliser un modèle pour créer le modèle d'événement, procédez comme suit :
 - A. Sélectionnez Event pattern form (Formulaire de modèle d'événement).
 - B. Pour Event source (Origine de l'événement), choisissez AWS services (Services).
 - C. Pour AWS Service, choisissez EC2.
 - D. Pour Event type (Type d'événement), choisissez EC2 AMI State Change (Modification de l'état d'AMI EC2).
 - E. Pour personnaliser le modèle, choisissez Edit pattern (Modifier le modèle) et apportez vos modifications pour correspondre à l'exemple de modèle d'événement.

- ii. Pour spécifier un modèle d'événement personnalisé, procédez comme suit :
 - A. Choisissez Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]).
 - B. Dans la boîte de dialogue Event pattern (Modèle d'événement), ajoutez le modèle d'événement pour cet exemple.
- c. Choisissez Next (Suivant).
5. Pour Select target(s) (Sélectionner la ou les cibles), procédez comme suit :
 - a. Pour Types de cibles, choisissez service AWS .
 - b. Pour Select a target (Sélectionner une cible), sélectionnez SNS topic (Rubrique SNS) pour envoyer un e-mail, un SMS ou une notification push mobile lorsque l'événement se produit.
 - c. Pour Topic (Rubrique), sélectionnez une rubrique existante. Vous devez d'abord créer une rubrique Amazon SNS à l'aide de la console Amazon SNS. Pour plus d'informations, consultez la section [Utilisation d'Amazon SNS pour la messagerie application-to-person \(A2P\) dans le manuel](#) du développeur Amazon Simple Notification Service.
 - d. (Facultatif) Sous Additional settings (Paramètres supplémentaires), vous pouvez configurer des paramètres supplémentaires. Pour plus d'informations, consultez la section [Création de EventBridge règles Amazon réagissant aux événements](#) (étape 16) dans le guide de EventBridge l'utilisateur Amazon.
 - e. Choisissez Suivant.
6. (Facultatif) Pour Tags (Identifications), vous pouvez également attribuer une ou plusieurs identifications à votre règle, puis choisir Next (Suivant).
7. Pour Review and create (Vérifier et créer), procédez comme suit :
 - a. Consultez les détails de la règle et modifiez-les si nécessaire.
 - b. Choisissez Créer une règle.

Pour plus d'informations, consultez les rubriques suivantes du guide de EventBridge l'utilisateur Amazon :

- [EventBridge Événements Amazon](#)
- [Modèles d' EventBridge événements Amazon](#)
- [EventBridge Règles Amazon](#)

Pour un didacticiel sur la création d'une fonction Lambda et d'une EventBridge règle qui exécute la fonction Lambda, consultez [Tutoriel : enregistrez l'état d'une instance Amazon EC2 à l'aide du manuel du développeur](#). EventBridge AWS Lambda

Comprendre les informations de facturation d'AMI

Il existe de nombreuses Amazon Machine Images (AMI) entre lesquelles choisir lorsque vous lancez vos instances, et celles-ci prennent en charge une variété de fonctionnalités et de plateformes du système d'exploitation. Pour comprendre comment l'AMI que vous choisissez lors du lancement de votre instance affecte le résultat net de votre AWS facture, vous pouvez rechercher la plate-forme du système d'exploitation et les informations de facturation associées. Faites ceci avant de lancer des instances Spot ou à la demande, ou d'acheter une Instance réservée.

Voici deux exemples qui illustrent en quoi une recherche préalable de votre AMI peut vous aider à choisir l'AMI qui correspond le mieux à vos besoins :

- Pour les Instances Spot, vous pouvez utiliser les détails de la plateforme sur l'AMI pour confirmer que l'AMI est prise en charge pour les Instances Spot.
- Lorsque vous achetez une Instance réservée, vous pouvez vous assurer que vous sélectionnez la plateforme du système d'exploitation (Platform) qui correspond aux détails de la plateforme sur l'AMI.

Pour plus d'informations sur la tarification des instances, consultez [Tarification Amazon EC2](#).

Sommaire

- [Champs d'informations de facturation d'AMI](#)
- [Recherche des détails de facturation et d'utilisation d'AMI](#)
- [Vérifier les frais d'AMI sur votre facture](#)

Champs d'informations de facturation d'AMI

Les champs suivants fournissent les informations de facturation associées à une AMI :

Platform details (Détails de la plateforme)

Détails de la plateforme associée au code de facturation de l'AMI. Par exemple, Red Hat Enterprise Linux.

Usage operation (Opération d'utilisation)

Opération de l'instance Amazon EC2 et code de facturation associé à l'AMI. Par exemple, RunInstances:0010. L'opération d'utilisation correspond à la colonne [LineItem/Operation](#) de votre rapport sur les AWS coûts et l'utilisation (CUR) et dans l'API [AWS Price List](#).

Vous pouvez consulter ces champs sur la page Instances ou AMI de la console Amazon EC2, ou dans la réponse renvoyée par la commande [describe-images](#). [Get-EC2Image](#)

Exemples de données : opération d'utilisation par plateforme

Le tableau suivant répertorie certains détails de la plateforme et les valeurs des opérations d'utilisation qui peuvent être affichés sur les pages Instances ou AMI de la console Amazon EC2, ou dans la réponse renvoyée par la commande [describe-images](#). [Get-EC2Image](#)

Platform details (Détails de la plateforme)	Opération d'utilisation ²
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0 ³
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110

Platform details (Détails de la plateforme)	Opération d'utilisation ²
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise ¹	RunInstances:0102
Windows with SQL Server Standard ¹	RunInstances:0006
Windows with SQL Server Web ¹	RunInstances:0202

¹ Si deux licences logicielles sont associées à une AMI, le champ Détails de la plate-forme indique les deux.

² Si vous utilisez des instances Spot, la valeur de votre rapport [lineitem/Operation](#) sur les AWS coûts et l'utilisation peut être différente de la valeur de l'opération d'utilisation répertoriée ici. Par exemple, s'il s'[lineitem/Operation](#) affiche `RunInstances:0010:SV006`, cela signifie qu'Amazon EC2 exécute Red Hat Enterprise Linux Spot Instance-Hour dans l'est des États-Unis (Virginie du Nord) dans la zone 6.

³ Cela apparaît comme RunInstances (Linux/UNIX) dans vos rapports d'utilisation.

Recherche des détails de facturation et d'utilisation d'AMI

Dans la console Amazon EC2, vous pouvez afficher les informations de facturation d'AMI à partir des pages AMI ou Instances. Vous pouvez également trouver des informations de facturation à l'aide du AWS CLI ou du service de métadonnées de l'instance.

Les champs suivants peuvent vous aider à vérifier les frais d'AMI sur votre facture :

- Platform details (Détails de la plateforme)
- Usage operation (Opération d'utilisation)
- ID D'AMI

Rechercher les informations de facturation d'AMI (console)

Procédez comme suit pour afficher les informations de facturation d'AMI dans la console Amazon EC2 :

Rechercher les informations de facturation d'AMI à partir de la page AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez AMI, puis sélectionnez une AMI.
3. Sous l'onglet Détails (Détails) vérifiez les valeurs de Platform details (Détails de la plateforme) et Usage operation (Opération d'utilisation).

Rechercher les informations de facturation d'AMI à partir de la page Instances

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances, puis sélectionnez l'instance.
3. Sous l'onglet Détails (ou l'onglet Description si vous utilisez la version antérieure de la console), examinez les valeurs pour Détails de la plateforme et Opération d'utilisation.

Rechercher les informations de facturation d'AMI (AWS CLI)

Pour trouver les informations de facturation de l'AMI à l'aide du AWS CLI, vous devez connaître l'ID de l'AMI. Si vous ne connaissez pas l'ID d'AMI, vous pouvez l'obtenir à partir de l'instance à l'aide de la commande [describe-instances](#).

Pour trouver l'ID d'AMI

Si vous connaissez l'ID d'instance, vous pouvez obtenir l'ID d'AMI de l'instance à l'aide de la commande [describe-instances](#).

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

Dans la sortie, l'ID d'AMI est spécifié dans le champ ImageId.

```
... "Instances": [  
  {  
    "AmiLaunchIndex": 0,  
    "ImageId": "ami-0123456789EXAMPLE",  
    "InstanceId": "i-123456789abcde123",  
    ...  
  }  
]
```

Pour trouver les informations de facturation d'AMI

Si vous connaissez l'ID d'AMI, vous pouvez utiliser la commande [describe-images](#) pour obtenir les détails de la plateforme d'AMI et de l'opération d'utilisation.

```
$ aws ec2 describe-images --image-ids ami-0123456789EXAMPLE
```

L'exemple de sortie suivant montre les champs PlatformDetails et UsageOperation. Dans cet exemple, la plateforme ami-0123456789EXAMPLE est Red Hat Enterprise Linux, et la valeur de l'opération d'utilisation et du code de facturation est RunInstances:0010.

```
{  
  "Images": [  
    {  
      "VirtualizationType": "hvm",  
      "Description": "Provided by Red Hat, Inc.",  
      "Hypervisor": "xen",  
      "EnaSupport": true,  
      "SriovNetSupport": "simple",  
      "ImageId": "ami-0123456789EXAMPLE",  
      "State": "available",  
      "BlockDeviceMappings": [  
        {
```

```
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "SnapshotId": "snap-111222333444aaabb",
            "DeleteOnTermination": true,
            "VolumeType": "gp2",
            "VolumeSize": 10,
            "Encrypted": false
        }
    },
    ],
    "Architecture": "x86_64",
    "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
    "RootDeviceType": "ebs",
    "OwnerId": "123456789012",
    "PlatformDetails": "Red Hat Enterprise Linux",
    "UsageOperation": "RunInstances:0010",
    "RootDeviceName": "/dev/sda1",
    "CreationDate": "2019-05-10T13:17:12.000Z",
    "Public": true,
    "ImageType": "machine",
    "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
}
]
}
```

Vérifier les frais d'AMI sur votre facture

Pour vous assurer de ne pas encourir de coûts imprévus, vous pouvez vérifier que les informations de facturation d'une instance figurant dans votre rapport sur les AWS coûts et l'utilisation (CUR) correspondent aux informations de facturation associées à l'AMI que vous avez utilisée pour lancer l'instance.

Pour vérifier les informations de facturation, recherchez l'ID d'instance dans votre rapport de coût et d'utilisation et vérifiez la valeur correspondante dans la colonne [lineitem/Operation](#). La valeur doit correspondre à la valeur de Usage operation (Opération d'utilisation) associée à l'AMI.

Par exemple, l'AMI `ami-0123456789EXAMPLE` contient les informations de facturation suivantes :

- Platform details (Détails de la plateforme = Red Hat Enterprise Linux
- Opération d'utilisation = RunInstances:0010

Si vous avez lancé une instance à l'aide de cette AMI, vous pouvez trouver l'ID d'instance dans votre rapport d'utilisation et de coût et vérifier la valeur correspondante dans la colonne [lineitem/Operation](#). Dans cet exemple, la valeur devrait être `RunInstances:0010`.

Quotas d'AMI

Les quotas suivants s'appliquent à la création et au partage des AMI. Les quotas s'appliquent par Région AWS.

Nom du quota	Description	Quota par défaut par région
AMI	Le nombre maximum des AMI publiques et privées autorisées par région. Cela inclut les AMI disponibles et en attente, ainsi que les AMI se trouvant dans la corbeille.	50 000
AMI publiques	Le nombre maximum d'AMI publiques, y compris les AMI publiques de la corbeille, autorisées par région.	5
Partage d'AMI	Le nombre maximum d'entités (organisations, unités d'organisation (UO) et comptes) avec lesquelles une AMI peut être partagée dans une région. Notez que si vous partagez une AMI avec une organisation ou une UO, le nombre de comptes dans l'organisation ou l'UO ne compte pas dans le quota.	1 000

Si vous dépassez vos quotas et que vous voulez créer ou partager d'autres AMI, vous pouvez effectuer les opérations suivantes :

- Si vous dépassez votre quota total d'AMI ou d'AMI publiques, pensez à annuler l'enregistrement des images inutilisées.
- Si vous dépassez votre quota pour les AMI publiques, pensez à rendre une ou plusieurs AMI publiques privées.
- Si vous dépassez votre quota de partage d'AMI, envisagez de partager vos AMI avec une organisation ou une UO au lieu de comptes séparés.
- Demandez une augmentation de quota pour les AMI.

Demande d'une augmentation de quota pour les AMI

Si vous avez besoin de plus que le quota par défaut pour les AMI, vous pouvez demander une augmentation de quota.

Pour demander une augmentation de quota pour les AMI

1. Ouvrez la console Service Quotas à l'adresse <https://console.aws.amazon.com/servicequotas/>.
2. Dans le panneau de navigation, choisissez Services AWS .
3. Choisissez Amazon Elastic Compute Cloud (Amazon EC2) dans la liste ou saisissez le nom du service dans le champ de recherche.
4. Choisissez le quota d'AMI pour demander une augmentation. Les quotas d'AMI que vous pouvez sélectionner sont les suivants :
 - AMI
 - AMI publiques
 - Partage d'AMI
5. Choisissez Request quota increase (Demander une augmentation de quota).
6. Pour Change quota value (Modifier la valeur du quota), saisissez la nouvelle valeur du quota, puis sélectionnez Request (Demander).

Pour afficher les demandes en attente ou récemment résolues, choisissez Dashboard (Tableau de bord) dans le volet de navigation. Pour les demandes en attente, choisissez l'état de la demande pour ouvrir le reçu de la demande. L'état initial d'une demande est Pending (En attente). Une fois que le statut est passé à Quota requested (Quota demandé), vous verrez le numéro du cas sous Support Center case number (Numéro de cas du centre de support). Choisissez le numéro de dossier pour ouvrir le billet pour votre demande.

Une fois la demande résolue, la Applied quota value (Valeur de quota appliquée) pour le quota est définie selon la nouvelle valeur.

Pour plus d'informations, consultez le [Guide de l'utilisateur Service Quotas](#).

instances Amazon EC2

Avant que vous ne lanciez un environnement de production, vous devez répondre aux questions suivantes.

Q. Quel type d'instance répond le mieux à mes besoins ?

Amazon EC2 fournit différents types d'instance pour vous permettre de choisir les capacités d'UC, de mémoire, de stockage et de mise en réseau dont vous avez besoin pour exécuter vos applications. Pour plus d'informations, consultez [Types d'instances Amazon EC2](#).

Q. Quelle option d'achat répond le mieux à mes besoins ?

Amazon EC2 prend en charge les instances à la demande (instances par défaut), les instances Spot et les instances réservées. Pour plus d'informations, consultez [Options d'achat d'instance](#).

Q. Quel type de volume racine répond à mes besoins ?

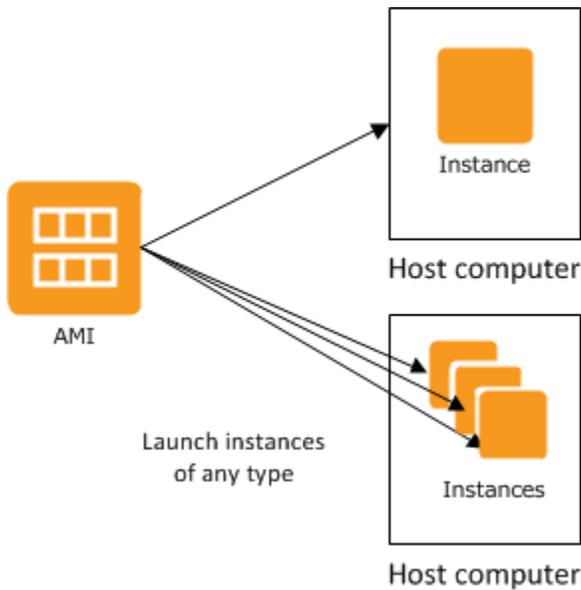
Chaque instance est basée sur Amazon EBS ou sur le stockage d'instances. Sélectionnez une AMI en fonction du type de volume racine dont vous avez besoin. Pour plus d'informations, consultez [Stockage pour le périphérique racine](#).

Q. Can I remotely manage a fleet of EC2 instances and machines in my hybrid environment ?(Q. Est-ce que je peux gérer à distance une flotte d'instances EC2 de machines dans mon environnement hybride ?)

AWS Systems Manager vous permet de gérer à distance et en toute sécurité la configuration de vos instances Amazon EC2, ainsi que de vos instances sur site et de vos machines virtuelles (VM) dans des environnements hybrides, y compris les machines virtuelles d'autres fournisseurs de cloud. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Systems Manager](#).

instances et AMI

Une Amazon Machine Image (AMI) est un modèle qui contient une configuration logicielle (par exemple, un système d'exploitation, un serveur d'applications et des applications). À partir d'une AMI, vous lancez une instance qui est une copie de l'AMI s'exécutant en tant que serveur virtuel dans le cloud. Vous pouvez lancer plusieurs instances d'une AMI, comme illustré sur la figure suivante.



Vos instances continuent de s'exécuter jusqu'à ce que vous les arrêtez, les mettiez en veille prolongée ou les résilieez, ou jusqu'à ce qu'elles connaissent une défaillance. En cas de défaillance d'une instance, vous pouvez en lancer une nouvelle à partir de l'AMI.

instances

Une instance est un serveur virtuel dans le cloud . Sa configuration au moment du lancement est une copie de l'AMI que vous avez spécifiée quand vous avez lancé l'instance.

Vous pouvez lancer différents types d'instance à partir d'une seule AMI. Un type d'instance détermine essentiellement les capacités matérielles de l'ordinateur hôte utilisé pour votre instance. Chaque type d'instance offre des capacités de calcul et de mémoire différentes. Sélectionnez un type d'instance en fonction de la quantité de mémoire et de la puissance de calcul dont vous avez besoin pour l'application ou le logiciel que vous prévoyez d'exécuter sur l'instance. Pour obtenir des spécifications détaillées sur les types d'instances, consultez les [spécifications](#) du guide des types d'instances Amazon EC2. Pour plus d'informations sur les tarifs, consultez la section Tarification [à la demande d'Amazon EC2](#).

Une fois une instance lancée, celle-ci ressemble à un hôte classique et vous pouvez interagir avec elle comme avec n'importe quel ordinateur. Vous exercez un contrôle total sur vos instances. Vous pouvez utiliser sudo pour exécuter des commandes nécessitant des privilèges racine.

Le nombre d'instances que vous pouvez exécuter est limité sur votre AWS compte. Pour plus d'informations sur cette limite et savoir comment demander que celle-ci soit augmentée, consultez

[Combien d'instances puis-je exécuter dans Amazon EC2](#) dans la questions fréquentes (FAQ) générale sur Amazon EC2.

Stockage pour votre instance

Le périphérique racine pour votre instance contient l'image utilisée pour démarrer l'instance. L'appareil racine est un volume Amazon Elastic Block Store (Amazon EBS) ou un volume de stockage d'instances. Pour plus d'informations, consultez [Volume racine de l'instance Amazon EC2](#).

Votre instance peut inclure des volumes de stockage local, appelés volumes de stockage d'instances, que vous pouvez configurer au moment du lancement avec la fonctionnalité de mappage de périphérique de stockage en mode bloc. Pour plus d'informations, consultez [Mappages de périphériques de stockage en mode bloc](#). Une fois que ces volumes ont été ajoutés et mappés à votre instance, ils sont à votre disposition pour être montés et utilisés. Si votre instance est défectueuse, ou si elle est arrêtée ou terminée, les données sur ces volumes sont perdues. Ces volumes sont donc mieux adaptés aux données temporaires. Pour maintenir en sécurité des données importantes, vous devez utiliser une stratégie de réplication sur plusieurs instances ou stocker vos données persistantes sur des volumes Amazon S3 ou Amazon EBS. Pour plus d'informations, consultez [Options de stockage pour vos instances Amazon EC2](#).

Bonnes pratiques de sécurité

- Utilisez AWS Identity and Access Management (IAM) pour contrôler l'accès à vos AWS ressources, y compris à vos instances. Pour plus d'informations, consultez [Identity and Access Management pour Amazon EC2](#).
- Limitez l'accès en permettant uniquement aux hôtes et réseaux approuvés d'accéder à des ports sur votre instance. Par exemple, vous pouvez restreindre l'accès SSH en limitant le trafic entrant sur le port 22. Pour plus d'informations, consultez [Groupes de sécurité Amazon EC2 pour vos instances EC2](#).
- Vérifiez régulièrement les règles de vos groupes de sécurité et veillez à appliquer le principe du moindre privilège—en donnant accès uniquement aux permissions dont vous avez besoin. Vous pouvez également créer différents groupes de sécurité pour gérer les instances ayant des exigences de sécurité différentes. Envisagez de créer un groupe de sécurité bastion qui autorise les connexions externes et conservez le reste de vos instances dans un groupe n'autorisant pas les connexions externes.
- Désactivez les connexions basées sur mot de passe pour les instances lancées à partir de votre AMI. Les mots de passe peuvent être trouvés ou craqués et représentent donc un risque pour la sécurité. Pour plus d'informations, consultez [Désactivation des connexions distantes basées sur](#)

[un mot de passe pour l'utilisateur root](#). Pour plus d'informations sur comment partager des AMI en toute sécurité, consultez [AMI partagées](#).

Arrêter et résilier des instances

Vous pouvez arrêter ou mettre fin à une instance en cours d'exécution à tout moment.

Arrêter une instance

Lorsqu'une instance est arrêtée, celle-ci exécute une fermeture normale, puis passe à un état `stopped`. Tous ses volumes Amazon EBS restent attachés et vous pouvez redémarrer l'instance ultérieurement.

L'utilisation d'instance supplémentaire ne vous est pas facturée pendant que l'instance est à un état arrêté. Vous êtes facturé pour chaque transition d'un état arrêté à un état en cours d'exécution. Si le type d'instance a changé alors que l'instance était arrêtée, le tarif du nouveau type d'instance vous est facturé après le démarrage de l'instance. Vous êtes également facturé pour le stockage Amazon EBS associé à votre instance, y compris le volume du périphérique racine.

Lorsqu'une instance est à l'état arrêté, vous pouvez attacher ou détacher des volumes Amazon EBS. Vous pouvez également créer une AMI à partir de l'instance, et vous pouvez modifier le noyau, le disque RAM et le type d'instance.

Résilier une instance

Lorsque vous mettez fin à une instance, celle-ci procède à une fermeture normale. Le volume du périphérique racine est supprimé par défaut, mais tous les volumes Amazon EBS attachés sont conservés par défaut, selon le paramètre de l'attribut `deleteOnTermination` de chaque volume. L'instance proprement dite est également supprimée et vous ne pourrez pas la redémarrer ultérieurement.

Pour éviter toute fin accidentelle, vous pouvez désactiver la possibilité de mettre fin à une instance. Dans ce cas, assurez-vous que l'attribut `disableApiTermination` est défini sur `true` pour l'instance. Pour contrôler le comportement de la fermeture d'une instance, par exemple, `shutdown -h` sous Linux ou `shutdown` sous Windows, définissez l'attribut de l'instance `instanceInitiatedShutdownBehavior` sur `stop` ou `terminate` en fonction des besoins. Les instances avec des volumes Amazon EBS pour le périphérique racine ont par défaut la valeur `stop`, et les instances avec des périphériques racine de stockage d'instance sont toujours terminés suite à une fermeture d'instance.

Pour plus d'informations, consultez [Cycle de vie d'une instance](#).

Note

Certaines AWS ressources, telles que les volumes Amazon EBS et les adresses IP Elastic, sont facturées quel que soit l'état de l'instance. Pour plus d'informations, consultez [Éviter les frais inattendus](#) dans le Guide de l'utilisateur AWS Billing . Pour plus d'informations sur les coûts Amazon EBS, consultez la [Tarification Amazon EBS](#).

AMI

Amazon Web Services (AWS) publie des Amazon Machine Images (AMI) qui contiennent des configurations logicielles courantes destinées à un usage public. En outre, les membres de la communauté des AWS développeurs ont publié leurs propres AMI personnalisées. Vous pouvez également créer vos propres AMI personnalisées ; cela vous permet de démarrer rapidement et facilement de nouvelles instances dotées de tout ce dont vous avez besoin. Par exemple, si votre application est un site web ou un service web, votre AMI peut inclure un serveur web, le contenu statique associé et le code pour les pages dynamiques. Ainsi, quand vous lancez une instance à partir de cette AMI, votre serveur web démarre et votre application est prête à accepter des demandes.

Toutes les AMI sont classées comme étant basées sur Amazon EBS, ce qui signifie que le périphérique racine pour une instance lancée à partir de l'AMI est un volume Amazon EBS, ou basée sur un stockage d'instances, ce qui signifie que le périphérique racine pour une instance lancée à partir de l'AMI est un volume de stockage d'instances créé à partir d'un template stocké dans Amazon S3.

La description d'une AMI indique le type de périphérique racine (ebs ou instance store). Ceci est important, car ce que vous pouvez faire avec chaque type d'AMI présente des différences significatives. Pour plus d'informations sur ces différences, consultez [Stockage pour le périphérique racine](#).

Vous pouvez annuler l'inscription de votre AMI lorsque vous avez terminé de l'utiliser. Après cette opération, vous ne pouvez pas utiliser l'AMI pour lancer de nouvelles instances. Les instances existantes lancées à partir de l'AMI ne sont pas affectées. Par conséquent, si vous avez également terminé avec les instances lancées à partir de ces AMI, vous devez les arrêter.

Types d'instances Amazon EC2

Lorsque vous lancez une instance, le type d'instance que vous spécifiez détermine les capacités matérielles de l'ordinateur hôte utilisé pour votre instance. Chaque type d'instance propose différentes capacités de calcul, de mémoire et de stockage, et est regroupé dans une famille de l'instance en fonction de ces capacités. Sélectionnez un type d'instance en fonction des exigences de l'application ou du logiciel que vous prévoyez d'exécuter sur votre instance.

Amazon EC2 dédie certaines ressources de l'ordinateur hôte, comme le CPU, la mémoire et le stockage d'instance, à une instance en particulier. Amazon EC2 partage d'autres ressources de l'ordinateur hôte, comme le réseau et le sous-système de disque, entre les instances. Si chaque instance d'un ordinateur hôte essaie d'utiliser autant que possible de l'une de ces ressources partagées, chacun reçoit une part égale de cette ressource. Cependant, quand une ressource est sous-utilisée, une instance peut consommer une part plus importante de cette ressource, tant qu'elle est disponible.

Chaque type d'instance offre des performances minimales plus ou moins élevées à partir d'une ressource partagée. Par exemple, les types d'instance avec des performances d'I/O élevées bénéficient d'une plus grande allocation de ressources partagées. L'allocation d'une plus grande part de ressources partagées réduit aussi les écarts de performances d'I/O. Pour la plupart des applications, des performances d'I/O modérées sont plus que suffisantes. Cependant, pour les applications qui requièrent des performances d'I/O plus élevées ou plus régulières, envisagez un type d'instance avec des performances d'I/O supérieures.

Sommaire

- [Types d'instance disponibles](#)
- [Spécifications matérielles](#)
- [Types de virtualisation AMI](#)
- [Rechercher un type d'instance Amazon EC2](#)
- [Obtenir des recommandations pour un type d'instance](#)
- [Modifier le type d'instance](#)
- [Instance de performance à capacité extensible](#)
- [Accélération des performances grâce aux instances de GPU](#)

Types d'instance disponibles

Amazon EC2 fournit un large choix de types d'instance optimisés pour différents cas d'utilisation. Les types d'instance incluent diverses combinaisons de capacité de processeur, de mémoire, de stockage et de mise en réseau et vous offrent la flexibilité nécessaire pour choisir les combinaisons de ressources les plus adaptées à vos applications. Chaque type d'instance inclut une ou plusieurs tailles d'instance, ce qui vous permet d'adapter vos ressources aux exigences de votre charge de travail cible. Pour plus d'informations sur les fonctionnalités et les cas d'utilisation, consultez les détails des [types d'instances Amazon EC2](#).

Conventions de dénomination des types d'instances

Les noms sont basés sur la famille d'instances, la génération, la famille de processeurs, les capacités et la taille. Pour plus d'informations, consultez les [conventions de dénomination](#) dans le guide des types d'instances Amazon EC2.

Rechercher un type d'instance

Pour déterminer quels types d'instances répondent à vos besoins, tels que les régions prises en charge, les ressources de calcul ou les ressources de stockage, consultez [Rechercher un type d'instance Amazon EC2](#) les [spécifications relatives aux types d'instances Amazon EC2 dans le guide des types](#) d'instances Amazon EC2.

instances de la génération actuelle

- Usage général : M5 | M5a | M5ad | M5dn | M5n | M5zn | M6a | M6g | M6gd | M6i | M6id | M6idn | M6in | M7a | M7g | M7GD | M7i | M7i-Flex | Mac1 | Mac2 | Mac2-M2 | Mac2-M2Pro T2 | T3 | T3 | T3 | T4
- Optimisé pour le calcul : C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6gd | C6gn | C6i | C6id | C6in | C7a | C7g | C7gd | C7gn | C7i | C7i-Flex
- Mémoire optimisée : R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6idn | R6in | R6id | R7a | R7g | R7i | R7iz | U-3TB1 | U-6TB1 | U-9TB1 | U-9TB1 | 12 To1 | U-18 TB1 | U-24 TB1 | U7 à 12 To | U7 à 16 To | U7 à 24 To | U7 à 32 To | X1 | x2GD | X2IDN | X2iEDN | X2ieZN | X1e | z1d
- Stockage optimisé : D2 | D3 | D3en | H1 | I3 | i3EN | i4G | i4i | iM4GN | IS4gen
- Calcul accéléré : DL1 | DL2q | F1 | G4ad | G4dn | G5 | G5g | G6 | Gr6 | Inf1 | Inf2 | P2 | P3 | P3dn | P4d | P4de | P5 | Trn1 | Trn1n | VT1

- Calcul à hautes performances : HPC6a | HPC6id | HPC7a | HPC7g

instances de la génération précédente

- Usage général : A1 | M1 | M2 | M3 | M4 | T1
- Optimisé pour le calcul : C1 | C3 | C4
- Mémoire optimisée : R3 | R4
- Stockage optimisé : I2
- Calcul accéléré : G3

Spécifications matérielles

Pour obtenir des spécifications détaillées sur les types d'instances, consultez les [spécifications](#) du guide des types d'instances Amazon EC2. Pour plus d'informations sur les tarifs, consultez la section Tarification [à la demande d'Amazon EC2](#).

Pour que vous puissiez déterminer le type d'instance qui correspond le mieux à vos besoins, nous vous recommandons de lancer une instance et d'utiliser votre propre application de comparaison. Comme vous payez l'instance à la seconde, il est pratique et économique de tester plusieurs types d'instances avant de prendre une décision. Si vos besoins évoluent, même après avoir pris une décision, vous pouvez par la suite modifier le type d'instance. Pour plus d'informations, consultez [Modifier le type d'instance](#).

Fonctions du processeur Intel

Les instances Amazon EC2 qui s'exécutent sur des processeurs Intel peuvent inclure les fonctions suivantes. Toutes les fonctions de processeur suivantes ne sont pas prises en charge par tous les types d'instance. Pour obtenir des informations détaillées sur les fonctionnalités disponibles pour chaque type d'instance, consultez la section Types d'[instances Amazon EC2](#).

- Jeu d'instructions Intel AES-NI — Le jeu d'instructions de chiffrement Intel AES-NI améliore l'algorithme Advanced Encryption Standard (AES) d'origine afin d'offrir une meilleure protection des données et une sécurité accrue. Toutes les instances EC2 de la génération actuelle prennent en charge cette fonction du processeur.
- Extensions Intel Advanced Vector (Intel AVX, Intel AVX2 et AVX-512) — Intel AVX et Intel AVX2 sont des extensions de jeux d'instructions 256 bits et Intel AVX-512 est une extension 512 bits,

toutes destinées aux applications exigeantes en matière de virgule flottante (FP). Les instructions Intel AVX améliorent les performances des applications telles que le traitement d'images et audio/vidéo, les simulations scientifiques, les analyses financières, ainsi que la modélisation et l'analyse 3D. Ces fonctions ne sont disponibles que sur les instances lancées avec des AMI HVM.

- Technologie Intel Turbo Boost — Les processeurs à technologie Intel Turbo Boost exécutent automatiquement les cœurs plus rapidement que la fréquence de fonctionnement de base.
- Intel Deep Learning Boost (Intel DL Boost) — Accélère les cas d'utilisation du deep learning d'IA. Les processeurs évolutifs Intel Xeon Scalable de 2e génération étendent Intel AVX-512 avec une nouvelle instruction de réseau neuronal vectoriel (VNNI/INT8) qui augmente considérablement les performances d'inférence du deep learning par rapport aux processeurs Intel Xeon Scalable de génération précédente (avec FP32), pour la reconnaissance/Oegmentation d'image, la détection d'objet, la reconnaissance vocale, la traduction, les systèmes de recommandation, l'apprentissage par renforcement, etc. VNNI peut ne pas être compatible avec toutes les distributions Linux.

Les instances suivantes prennent en charge VNNI : M5n, R5n, M5dn, M5zn, R5b, R5dn, D3, D3en et C6i. Les instances C5 et C5d prennent uniquement en charge VNNI pour les instances 12xlarge, 24xlarge et metal.

Les conventions d'appellation du secteur concernant les processeurs 64 bits peuvent donner lieu à une certaine confusion. Le fabricant de puces Advanced Micro Devices (AMD) a présenté la première architecture 64 bits commercialement viable basée sur le jeu d'instructions Intel x86. Par conséquent, ce type d'architecture est souvent appelé AMD64, quel que soit le fabricant. C'est notamment le cas pour Windows et plusieurs distributions Linux. C'est ce qui explique que les informations système internes d'une instance exécutée sur Ubuntu ou Windows indiquent une architecture de processeur AMD64, même quand les instances s'exécutent sur du matériel Intel.

AWS Processeurs Graviton

[AWS Graviton](#) est une famille de processeurs conçus pour offrir le meilleur rapport prix/performances pour vos charges de travail exécutées sur des instances Amazon EC2.

Pour plus d'informations, consultez [Getting started with Graviton](#).

AWS Trainium

Les instances alimentées par [AWS Trainium](#) sont spécialement conçues pour une formation en deep learning performante et rentable. Vous pouvez utiliser ces instances pour entraîner des modèles

de traitement du langage naturel, de vision par ordinateur et de recommandation utilisés dans un large éventail d'applications, telles que la reconnaissance vocale, la recommandation, la détection des fraudes et la classification d'images et de vidéos. Utilisez vos flux de travail existants dans des frameworks ML courants, tels que PyTorch et TensorFlow.

AWS Inférentie

Les instances alimentées par [AWS Inferentia](#) sont conçues pour accélérer l'apprentissage automatique. Ils fournissent une inférence d'apprentissage automatique à haute performance et à faible latence. Ces instances sont optimisées pour déployer des modèles de Deep Learning (DL) pour des applications telles que le traitement du langage naturel, la détection et la classification des objets, la personnalisation et le filtrage du contenu et la reconnaissance vocale.

Il y a plusieurs façons de démarrer :

- Use SageMaker, un service entièrement géré qui constitue le moyen le plus simple de démarrer avec les modèles d'apprentissage automatique. Pour plus d'informations, consultez [Get Started with SageMaker](#) dans le manuel Amazon SageMaker Developer Guide.
- Lancez une instance Inf1 ou Inf2 à l'aide de l'AMI Deep Learning. Pour plus d'informations, consultez la section [AWS Inferentia avec DLAMI](#) du Guide du développeur AWS Deep Learning AMI .
- Lancez une instance Inf1 ou Inf2 à l'aide de votre propre AMI et installez le [kit SDK AWS Neuron](#), qui vous permet de compiler, d'exécuter et de profiler des modèles de deep learning pour AWS Inferentia.
- Lancez une instance de conteneur à l'aide d'une instance Inf1 ou Inf2 et d'une AMI optimisée par Amazon ECS. Pour plus d'informations, consultez [AMI Amazon Linux 2 \(Inferentia\)](#) dans le Amazon Elastic Container Service Developer Guide.
- Créez un cluster Amazon EKS avec des nœuds exécutant des instances Inf1. Pour plus d'informations, consultez [Prise en charge d'Inferentia](#) dans le Guide de l'utilisateur Amazon EKS.

Types de virtualisation AMI

Le type de virtualisation de votre instance est déterminé par l'AMI que vous utilisez pour la lancer. Les types d'instance de la génération actuelle prennent uniquement en charge la virtualisation HVM. Certains types d'instances de la génération précédente prennent en charge les instances paravirtuelles (PV) et certaines AWS régions prennent en charge les instances PV. Pour plus d'informations, consultez [Types de virtualisation AMI](#).

Pour de meilleures performances, nous vous recommandons d'utiliser une AMI HVM. De plus, les AMI HVM sont obligatoires pour tirer parti de la mise en réseau améliorée. La virtualisation HVM utilise la technologie d'assistance matérielle fournie par la plate-forme. AWS Avec la virtualisation HVM, la machine virtuelle invitée s'exécute comme si elle se trouvait sur une plateforme matérielle native, si ce n'est qu'elle continue d'utiliser les pilotes du stockage et le réseau de la virtualisation PV pour des performances améliorées.

Rechercher un type d'instance Amazon EC2

Pour pouvoir lancer une instance, vous devez sélectionner un type d'instance à utiliser. Le type d'instance que vous choisissez peut dépendre des ressources requises par votre charge de travail, telles que les ressources de calcul, de mémoire ou de stockage. Il peut être utile d'identifier plusieurs types d'instance qui pourraient convenir à votre charge de travail et d'évaluer leurs performances dans un environnement de test. Rien ne remplace la mesure des performances de votre application sous charge.

Si vous avez déjà des instances EC2 en cours d'exécution, vous pouvez AWS Compute Optimizer obtenir des recommandations sur les types d'instances à utiliser pour améliorer les performances, économiser de l'argent, ou les deux. Pour plus d'informations, consultez [the section called "Pour les charges de travail existantes"](#).

Tâches

- [Rechercher un type d'instance à l'aide de la console](#)
- [Trouvez un type d'instance à l'aide du AWS CLI](#)

Rechercher un type d'instance à l'aide de la console

Vous pouvez trouver un type d'instance qui répond à vos besoins à l'aide de la console Amazon EC2.

Recherche d'un type d'instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région dans laquelle lancer vos instances. Vous pouvez sélectionner n'importe quelle région disponible, quel que soit votre emplacement.
3. Dans le volet de navigation, choisissez Types d'instances.
4. (Facultatif) Choisissez l'icône de préférences pour sélectionner les attributs de type d'instance à afficher, tels que la tarification Linux à la demande, puis choisissez Valider. Vous pouvez également sélectionner le nom d'un type d'instance pour ouvrir sa page de détails et afficher tous

les attributs disponibles dans la console. La console n'affiche pas tous les attributs disponibles via l'API ou la ligne de commande.

5. Utilisez les attributs de type d'instance pour filtrer la liste des types d'instance affichés uniquement aux types d'instance qui répondent à vos besoins. Par exemple, vous pouvez filtrer sur les attributs suivants :
 - Zones de disponibilité : le nom de la zone de disponibilité, de la zone locale ou des zones Wavelength. Pour plus d'informations, consultez [the section called "Régions et zones"](#).
 - vCPU ou Cores (Cœurs) : le nombre de vCPU ou de cœurs.
 - Mémoire (Gio) : la taille de la mémoire, en Gio.
 - Performances réseau : la performance du réseau, en Gigabits.
 - Stockage d'instance locale : indique si le type d'instance a un stockage d'instance local (`true` | `false`).
6. (Facultatif) Pour voir une side-by-side comparaison, cochez la case correspondant à plusieurs types d'instances. La comparaison s'affiche au bas de l'écran.
7. (Facultatif) Pour enregistrer la liste des types d'instance dans un fichier de valeurs séparées par des virgules (.csv) pour un examen plus approfondi, choisissez Actions, Download list CSV (Télécharger la liste CSV). Le fichier inclut tous les types d'instance qui correspondent aux filtres que vous avez définis.
8. (Facultatif) Pour lancer des instances en utilisant un type d'instance qui répond à vos besoins, cochez la case du type d'instance et choisissez Actions, Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Trouvez un type d'instance à l'aide du AWS CLI

Vous pouvez utiliser des AWS CLI commandes pour Amazon EC2 afin de trouver le type d'instance qui répond à vos besoins.

Pour rechercher un type d'instance à l'aide du AWS CLI

1. Si ce n'est pas déjà fait, installez le AWS CLI Pour plus d'informations, consultez le [guide de AWS Command Line Interface l'utilisateur](#).
2. Utilisez la commande [describe-instance-types](#) pour filtrer les types d'instance en fonction des attributs d'instance. Par exemple, vous pouvez utiliser la commande suivante pour afficher uniquement les types d'instance de la génération actuelle avec 64 GiB (65 536 MiB) de mémoire.

```
aws ec2 describe-instance-types --filters "Name=current-generation,Values=true"
"Name=memory-info.size-in-mib,Values=65536" --query "InstanceTypes[*].
[InstanceType]" --output text | sort
```

3. Utilisez la commande [describe-instance-type-offerings](#) pour filtrer les types d'instance proposés par emplacement (région ou zone). Par exemple, vous pouvez utiliser la commande suivante pour afficher les types d'instance proposés dans la zone spécifiée.

```
aws ec2 describe-instance-type-offerings --location-type "availability-
zone" --filters Name=location,Values=us-east-2a --region us-east-2 --query
"InstanceTypeOfferings[*].[InstanceType]" --output text | sort
```

4. Après avoir localisé les types d'instance qui répondent à vos besoins, enregistrez la liste afin de pouvoir utiliser ces types d'instance lorsque vous lancez des instances. Pour plus d'informations, consultez [Lancer votre instance](#) dans le Guide de l'utilisateur AWS Command Line Interface .

Obtenir des recommandations pour un type d'instance

Les outils suivants peuvent vous aider à sélectionner les types d'instances optimaux pour vos charges de travail nouvelles ou existantes :

- Nouvelles charges de travail : l'outil de recherche des types d'instance EC2 prend en compte votre cas d'utilisation, votre type de charge de travail, les préférences du fabricant du processeur, la façon dont vous hiérarchisez le prix et les performances, ainsi que les paramètres supplémentaires que vous pouvez spécifier. Il utilise ensuite ces données pour fournir des suggestions et des conseils concernant les types d'instances Amazon EC2 les mieux adaptés à vos nouvelles charges de travail.
- Charges de travail existantes : AWS Compute Optimizer analyse les spécifications de vos instances existantes et les indicateurs d'utilisation. Il utilise ensuite les données compilées pour recommander les types d'instances Amazon EC2 qui sont à même de gérer vos charges de travail existantes.

Obtention de recommandations sur le type d'instance

- [Obtention de recommandations sur le type d'instance pour une nouvelle charge de travail](#)
- [Obtention de recommandations sur le type d'instance pour une charge de travail existante](#)

Obtention de recommandations sur le type d'instance pour une nouvelle charge de travail

L'outil de recherche des types d'instance EC2 prend en compte votre cas d'utilisation, votre type de charge de travail, les préférences du fabricant du processeur, la façon dont vous hiérarchisez le prix et les performances, ainsi que les paramètres supplémentaires que vous pouvez spécifier. Il utilise ensuite ces données pour fournir des suggestions et des conseils concernant les types d'instances Amazon EC2 les mieux adaptés à vos nouvelles charges de travail.

Compte tenu du grand nombre de types d'instances disponibles, trouver les types d'instances adaptés à votre charge de travail peut s'avérer long et complexe. En utilisant l'outil de recherche de types d'instances EC2, vous pouvez rester à jour avec les derniers types d'instances et obtenir le meilleur rapport qualité-prix pour vos charges de travail.

Cette rubrique explique comment obtenir des suggestions et des conseils pour les types d'instances EC2 via la console Amazon EC2. Vous pouvez également consulter directement Amazon Q pour demander des conseils sur le type d'instance. Pour plus d'informations, consultez le [guide de l'utilisateur Amazon Q Developer](#).

Si vous recherchez des recommandations de type d'instance pour une charge de travail existante, utilisez AWS Compute Optimizer. Pour plus d'informations, consultez [Obtention de recommandations sur le type d'instance pour une charge de travail existante](#).

Utiliser l'outil de recherche de types d'instances EC2

Dans la console Amazon EC2, vous pouvez obtenir des suggestions de types d'instance à partir de l'outil de recherche de types d'instance EC2 dans l'assistant de lancement d'instance, lors de la création d'un modèle de lancement ou sur la page des types d'instances.

Suivez les instructions suivantes pour obtenir des suggestions et des conseils concernant les types d'instances EC2 à l'aide de l'outil de recherche de types d'instance EC2 de la console Amazon EC2. Pour visionner une animation des étapes, voir [Afficher une animation : obtenir des suggestions de types d'instance à l'aide de l'outil de recherche de types d'instance EC2](#).

Pour obtenir des suggestions de types d'instance à l'aide de l'outil de recherche de types d'instance EC2

1. Démarrez votre processus en utilisant l'une des méthodes suivantes :

- Suivez la procédure pour [lancer une instance](#). À côté de Type d'instance, cliquez sur le lien Obtenir des conseils.
 - Suivez la procédure pour [créer un modèle de lancement](#). À côté de Type d'instance, cliquez sur le lien Obtenir des conseils.
 - Dans le volet de navigation, choisissez Types d'instances, puis cliquez sur le bouton de recherche de types d'instances.
2. Dans l'écran Obtenir des conseils sur la sélection du type d'instance, procédez comme suit :
 - a. Spécifiez vos exigences en matière de type d'instance en sélectionnant des options pour le type de charge de travail, le cas d'utilisation, la priorité et les fabricants de processeurs.
 - b. (Facultatif) Pour définir des exigences plus détaillées pour votre charge de travail, procédez comme suit :
 - i. Développez les paramètres avancés.
 - ii. Pour ajouter un paramètre, sélectionnez-le, choisissez Ajouter et spécifiez une valeur pour le paramètre. Répétez l'opération pour chaque paramètre supplémentaire que vous souhaitez ajouter. Pour n'indiquer aucune valeur minimale ou maximale, laissez le champ vide.
 - iii. Pour supprimer un paramètre après l'avoir ajouté, cliquez sur le X à côté du paramètre.
 - c. Choisissez Obtenir des conseils sur le type d'instance.

Amazon EC2 vous propose des suggestions de familles d'instances correspondant à vos besoins spécifiques.
 3. Pour afficher les détails de chaque type d'instance au sein des familles d'instances suggérées, choisissez Afficher les détails de la famille d'instances recommandée.
 4. Sélectionnez un type d'instance qui répond à vos besoins, puis choisissez Actions, Lancer une instance ou Actions, Créer un modèle de lancement.

Sinon, si vous avez lancé le processus dans l'assistant de lancement d'instance ou sur la page du modèle de lancement, et que vous préférez revenir à votre flux d'origine, notez le type d'instance que vous souhaitez utiliser. Ensuite, dans l'assistant de lancement d'instance ou le modèle de lancement, dans Type d'instance, choisissez le type d'instance et terminez la procédure de lancement d'une instance ou de création d'un modèle de lancement.

Afficher une animation : obtenir des suggestions de types d'instance à l'aide de l'outil de recherche de types d'instance EC2

The screenshot displays the Amazon EC2 console interface. On the left is a navigation sidebar with categories like 'Instances', 'Images', 'Elastic Block Store', and 'Network & Security'. The main content area is divided into several panels:

- Resources:** A table showing the usage of various Amazon EC2 resources in the US East (N. Virginia) Region.

Resource	Count
Instances (running)	2
Dedicated Hosts	0
Instances	2
Load balancers	0
Security groups	12
Volumes	2
Auto Scaling Groups	0
Elastic IPs	0
Key pairs	0
Placement groups	0
Snapshots	3
- Launch instance:** A section with a 'Launch Instance' button and a 'Migrate a server' link. A note states: 'Note: Your instances will launch in the US East (N. Virginia) Region'.
- Service health:** Shows the 'AWS Health Dashboard' for the 'US East (N. Virginia)' region. The status is 'This service is operating normally.'.
- Account attributes:** Displays 'Default VPC' (vpc-92304aeb) and various settings like 'Data protection and security', 'Zones', and 'EC2 Serial Console'.
- Explore AWS:** Promotes 'Get Up to 40% Better Price Performance' for T4g instances and 'Enable Best Price-Performance with AWS Graviton2'.

Obtention de recommandations sur le type d'instance pour une charge de travail existante

AWS Compute Optimizer fournit des recommandations relatives aux instances Amazon EC2 pour vous aider à améliorer les performances, à économiser de l'argent, ou les deux. Vous pouvez utiliser ces recommandations pour décider de passer à un nouveau type d'instance.

Pour formuler des recommandations, Compute Optimizer analyse les spécifications et les métriques d'utilisation de vos instances existantes. Les données compilées sont ensuite utilisées pour recommander les types d'instances Amazon EC2 qui sont le plus à même de gérer la charge de travail existante. Les recommandations sont renvoyées avec la tarification horaire des instances.

Cette rubrique explique comment afficher les recommandations via la console Amazon EC2. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Compute Optimizer](#).

Note

Pour obtenir des recommandations de Compute Optimizer, vous devez d'abord vous inscrire à Compute Optimizer. Pour plus d'informations, consultez [Démarrer avec AWS Compute Optimizer](#) dans le Guide de l'utilisateur AWS Compute Optimizer .

Si vous recherchez des recommandations sur le type d'instance pour une nouvelle charge de travail, utilisez le sélecteur de type d'instance Amazon Q EC2. Pour plus d'informations, consultez [Obtention de recommandations sur le type d'instance pour une nouvelle charge de travail](#).

Table des matières

- [Limites](#)
- [Conclusions](#)
- [Afficher les recommandations](#)
- [Considérations relatives à l'évaluation des recommandations](#)
- [Ressources supplémentaires](#)

Limites

Compute Optimizer génère actuellement des recommandations pour les types d'instances C, D, H, I, M, R, T, X et z. Les autres types d'instance ne sont pas pris en compte par Compute Optimizer. Si vous utilisez d'autres types d'instances, ils ne seront pas répertoriés dans la vue des recommandations de Compute Optimizer. Pour plus d'informations sur les types d'instance pris en charge et non pris en charge, consultez la rubrique [Exigences pour les instances Amazon EC2](#) dans le Guide de l'utilisateur AWS Compute Optimizer .

Conclusions

Compute Optimizer classe ses résultats pour les instances EC2 comme suit :

- **Under-provisioned (Sous-allouée)** – Une instance EC2 est considérée comme sous-allouée lorsqu'au moins une spécification de votre instance (l'UC, la mémoire ou le réseau, par exemple) ne répond pas aux exigences de performances de votre charge de travail. Les instances EC2 sous-allouées peuvent entraîner des performances d'application médiocres.
- **Over-provisioned (Sur-allouée)** – Une instance EC2 est considérée comme sur-allouée lorsque la taille d'au moins une spécification de votre instance (l'UC, la mémoire ou le réseau, par exemple)

peut être réduite tout en répondant aux exigences de performances de votre charge de travail, et lorsqu'aucune spécification n'est sous-allouée. Les instances EC2 sur-allouées peuvent entraîner des coûts d'infrastructure inutiles.

- **Optimized (Optimisée)** – Une instance EC2 est considérée comme optimisée lorsque toutes les spécifications de votre instance (l'UC, la mémoire et le réseau, par exemple) répondent aux exigences de performances de votre charge de travail, et que l'instance n'est pas sur-allouée. Une instance EC2 optimisée exécute vos charges de travail avec des performances et des coûts d'infrastructure optimaux. Pour les instances optimisées, Compute Optimizer peut parfois recommander un type d'instance de nouvelle génération.
- **None (Aucune)** – Aucune recommandation n'est formulée pour cette instance. Cela peut se produire si vous êtes inscrit à Compute Optimizer depuis moins de 12 heures, ou lorsque l'instance s'exécute depuis moins de 30 heures, ou lorsque le type d'instance n'est pas pris en charge par Compute Optimizer. Pour plus d'informations, consultez [Limites](#) dans la section précédente.

Afficher les recommandations

Une fois que vous avez choisi Compute Optimizer, vous pouvez afficher les résultats qu'il génère pour vos instances EC2 dans la console EC2. Vous pouvez ensuite accéder à la console Compute Optimizer pour afficher les recommandations. Si vous vous êtes inscrit récemment, les résultats peuvent ne pas s'afficher dans la console EC2 avant 12 heures maximum.

Pour afficher une recommandation pour une instance EC2 via la console EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances, puis choisissez l'ID de l'instance .
3. Sur la page récapitulative de l'instance, dans la bannière AWS Compute Optimizer située en bas de la page, choisissez Afficher les détails.

L'instance s'ouvre dans Compute Optimizer, où elle est étiquetée comme instance Current (Actuelle) . Jusqu'à trois recommandations de type d'instance différentes, portant les noms Option 1, Option 2 et Option 3, sont fournies. La moitié inférieure de la fenêtre affiche les données CloudWatch métriques récentes pour l'instance actuelle : utilisation du processeur, utilisation de la mémoire, entrée réseau et sortie réseau.

4. (Facultatif) Dans la console Compute Optimizer, choisissez settings



pour modifier les colonnes visibles dans le tableau ou pour consulter les informations de

tarification publiques relatives à une option d'achat différente pour les types d'instances actuels et recommandés.

 Note

Si vous avez acheté une Instance réservée, votre instance à la demande peut être facturée au prix d'une Instance réservée. Avant de modifier votre type d'instance actuel, commencez par évaluer l'impact sur l'utilisation et la couverture de l'Instance réservée.

Déterminez si vous souhaitez utiliser l'une des recommandations. Décidez s'il convient d'améliorer les performances et/ou réduire les coûts. Pour plus d'informations, consultez [Affichage des recommandations de ressources](#) dans le Guide de l'utilisateur AWS Compute Optimizer .

Afficher les recommandations pour toutes les instances EC2 dans toutes les régions via la console Compute Optimizer

1. Ouvrez la console Compute Optimizer à l'adresse <https://console.aws.amazon.com/compute-optimizer/>.
2. Choisissez View recommendations for all EC2 instances (Afficher les recommandations pour toutes les instances EC2).
3. Vous pouvez effectuer les actions suivantes sur la page des recommandations :
 - a. Pour filtrer les recommandations relatives à une ou plusieurs AWS régions, entrez le nom de la région dans la zone de texte Filtrer par une ou plusieurs régions, ou choisissez une ou plusieurs régions dans la liste déroulante qui apparaît.
 - b. Pour afficher les recommandations relatives aux ressources d'un autre compte, choisissez Compte, puis sélectionnez un autre ID de compte.

Cette option n'est disponible que si vous êtes connecté au compte de gestion d'une organisation et que vous vous êtes inscrit à tous les comptes membres de l'organisation.

- c. Pour effacer les filtres sélectionnés, choisissez Annuler les filtres.
- d. Pour modifier l'option d'achat qui s'affiche pour les types d'instances actuels et recommandés, choisissez settings



puis choisissez Instances à la demande, Instances réservées, standard 1 an sans paiement initial, ou Instances réservées, standard 3 ans sans paiement initial.

- e. Pour afficher des détails, tels que des recommandations supplémentaires et une comparaison des métriques d'utilisation, choisissez le résultat (Under-provisioned (Sous-allouée), Over-provisioned (Sur-allouée) ou Optimized (Optimisée)) en regard de l'instance souhaitée. Pour plus d'informations, consultez [Affichage des détails de la ressource](#) dans le Guide de l'utilisateur AWS Compute Optimizer .

Considérations relatives à l'évaluation des recommandations

Avant de modifier un type d'instance, tenez compte des éléments suivants :

- Les recommandations ne prévoient pas votre utilisation. Les recommandations sont basées sur votre historique d'utilisation au cours de la période de 14 jours la plus récente. Veillez à choisir un type d'instance censé répondre à vos futurs besoins en termes de ressources.
- Concentrez-vous sur le graphique des métriques pour déterminer si l'utilisation réelle est inférieure à la capacité d'instance. Vous pouvez également consulter les données métriques (moyenne, pic, percentile) afin d'évaluer plus en détail les recommandations relatives CloudWatch à votre instance EC2. Par exemple, notez l'évolution des métriques de pourcentage d'UC pendant la journée et s'il y a des pics qui doivent être pris en compte. Pour plus d'informations, consultez la section [Affichage des métriques disponibles](#) dans le guide de CloudWatch l'utilisateur Amazon.
- Compute Optimizer peut fournir des recommandations pour les instances de performance à capacité extensible, à savoir les instances T3, T3a et T2. Si vous dépassez régulièrement le niveau de base, assurez-vous que vous pouvez continuer à le faire en fonction des vCPU du nouveau type d'instance. Pour plus d'informations, consultez [Concepts et définitions clés pour les instances de performance à capacité extensible](#).
- Si vous avez acheté une Instance réservée, votre instance à la demande peut être facturée au prix d'une Instance réservée. Avant de modifier votre type d'instance actuel, commencez par évaluer l'impact sur l'utilisation et la couverture de l'Instance réservée.
- Dans la mesure du possible, envisagez des conversions vers des instances de nouvelle génération.
- Lors de la migration vers une autre famille d'instances, assurez-vous que le type d'instance actuel et le nouveau type d'instance sont compatibles, en termes de virtualisation, d'architecture ou de type de réseau par exemple. Pour plus d'informations, consultez [Compatibilité pour modifier le type d'instance](#).
- Enfin, tenez compte de la note de risque de performances fournie pour chaque recommandation. Le risque de performances correspond à l'effort que vous pourriez avoir à consacrer pour valider si

le type d'instance recommandé répond aux exigences de performances de votre charge de travail. Nous recommandons également des tests rigoureux de charge et de performance avant et après toute modification.

Il existe d'autres considérations à prendre en compte lors du redimensionnement d'une instance EC2. Pour plus d'informations, consultez [Modifier le type d'instance](#).

Ressources supplémentaires

Pour plus d'informations, consultez:

- [Types d'instances Amazon EC2](#)
- [AWS Compute Optimizer Guide de l'utilisateur](#)

Modifier le type d'instance

Au fur et à mesure que vos besoins évoluent, il se peut que vous constatiez que votre instance est sur-utilisée (le type d'instance est trop petit) ou sous-utilisée (le type d'instance est trop grand). Si tel est le cas, vous pouvez redimensionner votre instance en modifiant son type d'instance. Par exemple, si votre instance `t2.micro` est trop petite pour sa charge de travail, vous pouvez augmenter sa taille en la remplaçant par un type d'instance T2 plus volumineux, comme `t2.large`. Vous pouvez également la remplacer par un autre type d'instance, par exemple `m5.large`. Vous pouvez également passer d'un type d'instance d'une génération précédente vers un type d'instance de génération actuelle pour tirer parti de certaines fonctions, telles que la prise en charge d'IPv6.

Si vous souhaitez une recommandation du type d'instance le mieux à même de gérer votre charge de travail existante, vous pouvez utiliser AWS Compute Optimizer. Pour plus d'informations, consultez [Obtention de recommandations sur le type d'instance pour une charge de travail existante](#).

Lorsque vous modifiez le type d'instance, vous commencez à payer le taux du nouveau type. Pour consulter les tarifs à la demande de tous les types d'instances, consultez la rubrique [Tarification à la demande d'Amazon EC2](#).

Pour ajouter du stockage supplémentaire à votre instance sans modifier le type d'instance, ajoutez-y un volume EBS. Pour plus d'informations, consultez la section [Attacher un volume Amazon EBS à une instance](#) dans le guide de l'utilisateur Amazon EBS.

Quelles sont les instructions à suivre ?

Il existe différentes instructions pour la modification du type d'instance. Les instructions à suivre dépendent du volume racine de l'instance et de la compatibilité du type d'instance avec la configuration actuelle de l'instance. Pour en savoir plus sur la façon dont la compatibilité est déterminée, consultez [Compatibilité pour modifier le type d'instance](#).

Utilisez le tableau suivant pour déterminer quelles instructions suivre.

Volume racine	Compatibilité	Suivez ces instructions
EBS	Compatible	Modifier le type d'instance d'une instance basée sur EBS
EBS	Non compatible	Modifier le type d'instance en lançant une nouvelle instance
Stockage d'instances	Ne s'applique pas	Modifier le type d'une instance basée sur le stockage d'instances

Considérations relatives aux types d'instances compatibles

Lors de la modification du type d'instance d'une instance existante, tenez compte des éléments suivants :

- Vous devez arrêter votre instance basée sur Amazon EBS avant de pouvoir modifier son type d'instance. Veillez à prévoir un temps d'arrêt pendant que votre instance est arrêtée. L'arrêt d'une instance et la modification de son type peuvent prendre quelques minutes, et la durée du redémarrage de votre instance peut varier en fonction des scripts de démarrage de votre application. Pour plus d'informations, consultez [Arrêtez et démarrez les instances Amazon EC2](#).
- Lorsque vous arrêtez et démarrez une instance, nous déplaçons l'instance vers un nouveau matériel. Si votre instance possède une adresse IPv4 publique, nous libérons l'adresse et attribuons à l'instance une nouvelle adresse IPv4 publique. Si vous avez besoin d'une adresse IPv4 publique qui ne change pas, utilisez une [adresse IP élastique](#).
- Vous ne pouvez pas modifier le type d'instance d'une [instance Spot](#).

- [Instances Windows] Nous vous recommandons de mettre à jour le package de pilotes AWS PV avant de modifier le type d'instance. Pour plus d'informations, consultez [the section called "Mettre à niveau les pilotes PV"](#).
- Si votre instance est dans un groupe Auto Scaling, le service Amazon EC2 Auto Scaling marque l'instance arrêtée comme étant non saine, et peut y mettre fin et lancer une instance de remplacement. Pour empêcher que cela ne se produise, vous pouvez suspendre les processus de mise à l'échelle pour le groupe pendant que vous modifiez le type d'instance. Pour plus d'informations, consultez [Suspension et reprise d'un processus pour un groupe Auto Scaling](#) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.
- Lorsque vous modifiez le type d'instance d'une instance avec des volumes de stockage d'instances NVMe, l'instance mise à jour peut avoir des volumes de stockage d'instances supplémentaires, car tous les volumes de stockage d'instances NVMe sont disponibles même s'ils ne sont pas spécifiés dans l'AMI ou le mappage de périphérique de stockage en mode bloc d'instances. Autrement, l'instance mise à jour a le même nombre de volumes de stockage d'instances que celui spécifié lors du lancement de l'instance initiale.
- Le nombre maximal de volumes Amazon EBS que vous pouvez associer à une instance dépend du type et de la taille de l'instance. Vous ne pouvez pas passer à un type ou à une taille d'instance qui ne prennent pas en charge le nombre de volumes déjà attachés à votre instance. Pour plus d'informations, consultez [Limites de volume d'instance](#).

Modifier le type d'instance d'une instance basée sur EBS

Suivez les instructions suivantes pour modifier le type d'instance d'une instance basée sur EBS si le type d'instance requis est compatible avec la configuration actuelle de l'instance.

Pour modifier le type d'instance d'une instance basée sur Amazon EBS

1. (Facultatif) Si le nouveau type d'instance requiert des pilotes qui ne sont pas installés sur l'instance existante, vous devez vous connecter à votre instance et installer les pilotes. Pour plus d'informations, consultez [Compatibilité pour modifier le type d'instance](#).
2. [Instances Windows] Si vous avez configuré votre instance Windows pour utiliser l'[adressage IP statique](#) et que vous passez d'un type d'instance qui ne prend pas en charge la mise en réseau améliorée à un type d'instance prenant en charge la mise en réseau améliorée, vous pouvez recevoir un avertissement concernant un conflit d'adresses IP potentiel lorsque vous reconfigurez l'adressage IP statique. Pour éviter ceci, activez DHCP sur l'interface réseau pour votre instance avant de modifier le type d'instance. Depuis votre instance, ouvrez le Centre

Réseau et partage, ouvrez Internet Protocol Version 4 (TCP/IPv4) Propriétés (Propriétés du Protocole Internet version 4 (TCP/IPv4)) pour l'interface réseau, puis choisissez Obtain an IP address automatically (Obtenir une adresse IP automatiquement). Modifiez le type d'instance et reconfigurez l'adressage IP statique sur l'interface réseau.

3. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
4. Dans le panneau de navigation, choisissez Instances.
5. Sélectionnez l'instance et choisissez Instance state (État de l'instance), Stop instance (Arrêter l'instance). Lorsque vous êtes invité à confirmer l'opération, choisissez Stop (Arrêter). L'arrêt de l'instance peut prendre quelques minutes.
6. Tandis que l'instance est toujours sélectionnée, choisissez Actions, Instance settings (Paramètres de l'instance), puis Change instance type (Changer le type d'instance). Cette action est grisée si l'état de l'instance n'est pas stopped.
7. Sur la page Change instance type (Modifier le type d'instance), procédez comme suit :

- a. Dans Instance type (Type d'instance), sélectionnez le type d'instance souhaité.

Si le type d'instance ne figure pas dans la liste, il n'est pas compatible avec la configuration de votre instance. Au lieu de cela, suivez les instructions suivantes : [Modifier le type d'instance en lançant une nouvelle instance](#).

- b. (Facultatif) Si le type d'instance que vous avez choisi prend en charge l'optimisation EBS, sélectionnez EBS-optimized (Optimisé pour EBS) pour activer l'optimisation EBS ou désélectionnez EBS-optimized (Optimisé pour EBS) pour la désactiver. Si le type d'instance que vous avez sélectionné est optimisé pour EBS par défaut, EBS-optimized (Optimisé pour EBS) est sélectionné et vous ne pouvez pas annuler la sélection.
 - c. Choisissez Apply (Appliquer) pour accepter les nouveaux paramètres.
8. Pour démarrer l'instance, sélectionnez l'instance et choisissez Instance state (État de l'instance), Start instance (Démarrer l'instance). Il peut s'écouler quelques minutes avant que l'instance ne passe à l'état running. Si votre instance ne démarre pas, consultez la section [Résoudre les problèmes de modification du type d'instance](#).
 9. [Instances Windows] Si votre instance exécute Windows Server 2016 ou Windows Server 2019 avec EC2Launch v1, connectez-vous à votre instance Windows et exécutez le PowerShell script EC2Launch suivant pour configurer l'instance une fois le type d'instance modifié.

⚠ Important

Le mot de passe de l'administrateur sera réinitialisé lorsque vous activerez le script d'initialisation de l'instance EC2 Launch. Vous pouvez modifier le fichier de configuration pour désactiver la réinitialisation du mot de passe administrateur en le spécifiant dans les paramètres des tâches d'initialisation. Pour savoir comment désactiver la réinitialisation du mot de passe, voir [Configurer les tâches d'initialisation](#) (EC2Launch) ou [Modifier les paramètres](#) (EC2Launch v2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -  
Schedule
```

Modifier le type d'instance en lançant une nouvelle instance

Si la configuration active de votre instance EBS est incompatible avec le nouveau type d'instance que vous souhaitez, vous ne pouvez pas modifier le type de l'instance d'origine. À la place, vous devez lancer une nouvelle instance dotée d'une configuration compatible avec le nouveau type d'instance souhaité, puis migrer votre application vers la nouvelle instance. Par exemple, si vous avez lancé votre instance d'origine à partir d'une AMI PV, mais que vous souhaitez passer à un type d'instance de génération actuelle nécessitant une AMI HVM, vous devrez lancer une nouvelle instance à partir d'une AMI HVM. Pour en savoir plus sur la façon dont la compatibilité est déterminée, consultez [Compatibilité pour modifier le type d'instance](#).

Pour migrer votre application vers une nouvelle instance, procédez comme suit :

- Sauvegardez les données de votre instance d'origine.
- Lancez une nouvelle instance ayant une configuration compatible avec le nouveau type d'instance que vous souhaitez et attachez tous les volumes EBS attachés à votre instance d'origine.
- Installez votre application et les logiciels sur la nouvelle instance.
- Restaurez toutes les données.
- Si votre instance d'origine a une adresse IP élastique et que vous souhaitez garantir que vos utilisateurs continuent à utiliser sans interruption les applications sur votre instance, vous devez associer l'adresse IP élastique à la nouvelle instance. Pour plus d'informations, consultez [Adresse IP élastique](#).

Pour modifier le type d'instance d'une nouvelle configuration d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sauvegardez les données que vous devez conserver, comme suit :
 - Pour les données qui se trouvent sur les volumes de stockage d'instances, sauvegardez-les dans un stockage permanent.
 - Pour les données de vos volumes EBS, créez un instantané des volumes ou détachez-les de l'instance afin de pouvoir les associer ultérieurement à la nouvelle instance.
3. Dans le panneau de navigation, sélectionnez Instances.
4. Sélectionnez Launch instances (Lancer des instances). Lorsque vous configurez l'instance, procédez comme suit :
 - a. Sélectionnez une AMI qui prendra en charge le type d'instance souhaité. Notez que les types d'instance de génération actuelle nécessitent une AMI HVM.
 - b. Sélectionnez le nouveau type d'instance souhaité. Si le type d'instance que vous souhaitez n'est pas disponible, il n'est pas compatible avec la configuration de l'AMI que vous avez sélectionnée.
 - c. Si vous utilisez une adresse IP élastique, sélectionnez le VPC dans lequel l'instance d'origine s'exécute.
 - d. Si vous voulez autoriser le même trafic pour atteindre la nouvelle instance, sélectionnez le groupe de sécurité associé à l'instance d'origine.
 - e. Une fois que vous avez terminé la configuration de votre nouvelle instance, effectuez les étapes pour sélectionner une paire de clés et lancer votre instance. Il peut s'écouler quelques minutes avant que l'instance ne passe à l'état `running`.
5. Si nécessaire, attachez les nouveaux volumes EBS en fonction des instantanés que vous avez créés, ou les volumes EBS que vous avez détachés de l'instance d'origine, à la nouvelle instance.
6. Installez votre application et les logiciels requis sur la nouvelle instance.
7. Restaurez les données que vous avez sauvegardées depuis les volumes de stockage d'instances de l'instance d'origine.
8. Si vous utilisez une adresse IP élastique, attribuez-la à la nouvelle instance comme suit :
 - a. Dans le volet de navigation, sélectionnez Elastic IPs (Adresses IP Elastic).

- b. Sélectionnez l'adresse IP Elastic associée à l'instance d'origine, choisissez Actions, puis Dissocier l'adresse IP Elastic. Sélectionnez Dissocier lorsque vous êtes invité à confirmer l'opération.
 - c. L'adresse IP Elastic étant toujours sélectionnée, choisissez Actions, puis Associer l'adresse IP Elastic.
 - d. Pour Resource type (Type de ressource), choisissez Instance.
 - e. Pour Instance, choisissez la nouvelle instance à laquelle vous souhaitez associer l'adresse IP élastique.
 - f. (Facultatif) Pour Private IP address (Adresse IP privée), spécifiez une adresse IP privée à laquelle associer l'adresse IP Elastic.
 - g. Choisissez Associate.
9. (Facultatif) Vous pouvez terminer l'instance d'origine si elle n'est plus nécessaire. Sélectionnez l'instance, vérifiez que vous êtes sur le point de résilier l'instance d'origine, et non la nouvelle instance (par exemple, vérifiez le nom ou l'heure du lancement), puis sélectionnez Instance state (État de l'instance), Terminate instance (Résilier l'instance).

Compatibilité pour modifier le type d'instance

Vous pouvez modifier le type d'instance uniquement si la configuration actuelle de l'instance est compatible avec le type d'instance souhaité. Si le type d'instance souhaité n'est pas compatible avec votre configuration actuelle d'instance, vous devez lancer une nouvelle instance dotée d'une configuration compatible avec le type d'instance, puis migrer votre application vers la nouvelle instance.

[Instances Linux] Vous pouvez utiliser le [AWSSupport-MigrateXenToNitroLinux](#) runbook pour migrer des instances Linux compatibles d'un type d'instance Xen vers un type d'instance Nitro. Pour plus d'informations, consultez [AWSSupport-MigrateXenToNitroLinux runbook](#) dans la référence AWS Systems Manager Automation runbook.

[Instances Windows] Pour obtenir des conseils supplémentaires sur la migration d'instances Windows compatibles d'un type d'instance Xen vers un type d'instance Nitro, voir [Migrer vers des types d'instances de dernière génération](#).

La compatibilité est déterminée de la manière suivante :

Type de virtualisation

Les AMI Linux utilisent l'un des deux types de virtualisation : virtualisation paravirtuelle (PV) ou virtualisation de machine virtuelle matérielle (HVM). Si une instance a été lancée depuis une AMI de virtualisation paravirtuelle, vous ne pouvez pas la changer en un type d'instance qui n'utilise que la virtualisation HVM. Pour plus d'informations, consultez [Types de virtualisation AMI](#). Pour vérifier le type de virtualisation de votre instance, consultez le champ Virtualization (Virtualisation) dans le panneau des détails de l'écran Instances dans la console Amazon EC2.

Architecture

Les AMI étant propres à l'architecture du processeur, vous devez sélectionner un type d'instance doté de la même architecture de processeur que le type d'instance actuel. Exemples :

- Si le type d'instance actuel est doté d'un processeur basé sur l'architecture Arm, vous êtes limité aux types d'instance qui prennent en charge un processeur basé sur l'architecture Arm, notamment C6g et M6g.
- Les types d'instances suivants sont les seuls qui prennent en charge les AMIs 32 bits : t2.nano, t2.micro, t2.small, t2.medium, c3.large, t1.micro, m1.small, m1.medium et c1.medium. Si vous modifiez le type d'une instance 32 bits, vous êtes limité à ces types d'instance.

Cartes réseau

Si vous passez d'un pilote d'une carte réseau à un autre, les paramètres de la carte réseau sont réinitialisés lorsque le système d'exploitation crée la nouvelle carte. Pour reconfigurer les paramètres, vous devrez peut-être accéder à un compte local doté d'autorisations d'administrateur. Voici des exemples de déplacement d'une carte réseau à une autre :

- AWS PV (instances T2) vers Intel 82599 VF (instances M4)
- Intel 82599 VF (la plupart des instances M4) vers ENA (instances M5)
- ENA (instances M5) vers ENA haute bande passante (instances M5n)

Cartes réseau

Certains types d'instance prennent en charge plusieurs [cartes réseau](#). Vous devez sélectionner un type d'instance prenant en charge le même nombre de cartes réseau que le type d'instance actuel.

Réseaux améliorés

Les types d'instance prenant en charge les [réseaux améliorés](#) nécessitent l'installation des pilotes requis. Par exemple, les [instances créées sur le système AWS Nitro](#) nécessitent des AMI

basées sur EBS avec les pilotes Elastic Network Adapter (ENA) installés. Pour passer d'un type d'instance qui ne prend pas en charge les réseaux améliorés à un type qui les prend en charge, vous devez installer les [pilotes ENA](#) ou les [pilotes ixgbevf](#) sur l'instance, selon le cas.

Note

Lorsque vous redimensionnez une instance avec ENA Express activé, le nouveau type d'instance doit également prendre en charge ENA Express. Pour obtenir la liste des types d'instance qui prennent en charge ENA Express, veuillez consulter [Types d'instance pris en charge pour ENA Express](#).

Pour passer d'un type d'instance qui prend en charge ENA Express à un type d'instance qui ne prend pas en charge ENA Express, assurez-vous qu'ENA Express n'est pas actuellement activé avant de redimensionner l'instance.

NVMe

Les volumes EBS sont exposés en tant que périphériques en mode bloc NVMe sur [des instances basées sur le système AWS Nitro](#). Si vous passez d'un type d'instance ne prenant pas en charge NVMe à un type d'instance prenant en charge NVMe, vous devez commencer par installer les pilotes NVMe sur votre instance. En outre, les noms des périphériques que vous spécifiez dans le mappage des périphériques par blocs sont renommés à l'aide des noms de périphériques NVMe (`/dev/nvme[0-26]n1`).

[Instances Linux] Par conséquent, pour monter des systèmes de fichiers au moment du démarrage/etc/fstab, vous devez utiliser l'UUID/label au lieu des noms de périphériques.

Limites de volume

Le nombre maximal de volumes Amazon EBS que vous pouvez associer à une instance dépend du type et de la taille de l'instance. Pour plus d'informations, consultez [Limites de volume d'instance](#).

Vous pouvez uniquement passer à un type ou à une taille d'instance qui prend en charge le même nombre ou un plus grand nombre de volumes que celui qui est actuellement attaché à l'instance. Si vous optez pour un type d'instance ou une taille d'instance qui ne prend pas en charge le nombre de volumes actuellement attachés, la demande échoue. Par exemple, si vous passez d'une instance `m7i.4xlarge` avec 32 volumes attachés à une instance `m6i.4xlarge`, qui prend en charge un maximum de 27 volumes, la demande échoue.

Résoudre les problèmes de modification du type d'instance

Utilisez les informations suivantes pour identifier et résoudre les problèmes que vous pouvez rencontrer lorsque vous modifiez le type d'instance.

L'instance ne démarre pas après avoir modifié le type d'instance

Cause possible : les exigences relatives au nouveau type d'instance ne sont pas satisfaites

Si votre instance ne démarre pas, il est possible qu'une des exigences pour le nouveau type d'instance n'ait pas été respectée. Pour plus d'informations, consultez la section relative à la [raison pour laquelle mon instance Linux ne démarre pas après que j'ai modifié son type](#).

Cause possible : l'AMI ne prend pas en charge le type d'instance

Si vous utilisez la console EC2 pour modifier le type d'instance, seuls les types d'instance pris en charge par l'AMI sélectionnée sont disponibles. Toutefois, si vous utilisez le AWS CLI pour lancer une instance, vous pouvez spécifier une AMI et un type d'instance incompatibles. Si l'AMI et le type d'instance sont incompatibles, l'instance ne peut pas démarrer. Pour plus d'informations, consultez [Compatibilité pour modifier le type d'instance](#).

Cause possible : l'instance se trouve dans un groupe de placement du cluster

Si votre instance se trouve dans un [groupe de placement du cluster](#) et, qu'après avoir modifié le type d'instance, l'instance ne démarre pas, essayez ce qui suit :

1. Arrêtez toutes les instances du groupe de placement du cluster.
2. Modifiez le type de l'instance en question.
3. Démarrez toutes les instances du groupe de placement du cluster.

L'application ou le site web n'est pas accessible depuis Internet après avoir modifié le type d'instance

Cause possible : l'adresse IPv4 publique est publiée

Lorsque vous modifiez le type d'instance, vous devez d'abord arrêter l'instance. Lorsque vous arrêtez une instance, nous libérons l'adresse IPv4 publique et attribuons à l'instance une nouvelle adresse.

Pour retenir l'adresse IPv4 publique entre les arrêts et les démarrages de l'instance, nous vous recommandons d'utiliser une adresse IP élastique, sans frais supplémentaires, à condition que votre instance soit en cours d'exécution. Pour plus d'informations, consultez [Adresses IP Elastic](#).

Modifier le type d'une instance basée sur le stockage d'instances

Une instance basée sur le stockage d'instances est une instance qui possède un volume racine de stockage d'instances. Vous ne pouvez pas modifier le type d'une instance qui possède un volume racine de stockage d'instances. À la place, vous devez créer une AMI à partir de votre instance, lancer une nouvelle instance à partir de cette AMI et sélectionner le type d'instance souhaité, puis migrer votre application vers la nouvelle instance. Notez que le type d'instance souhaité doit être compatible avec l'AMI que vous créez. Pour en savoir plus sur la façon dont la compatibilité est déterminée, consultez [Compatibilité pour modifier le type d'instance](#).

Présentation du processus

- Sauvegardez les données de votre instance d'origine.
- Créez une AMI à partir de votre instance d'origine.
- Lancez une nouvelle instance à partir de cette AMI et sélectionnez le type d'instance souhaité.
- Installez votre application sur la nouvelle instance.
- Si votre instance d'origine a une adresse IP élastique et que vous souhaitez garantir que vos utilisateurs continuent à utiliser sans interruption les applications sur votre instance, vous devez associer l'adresse IP élastique à la nouvelle instance. Pour plus d'informations, consultez [Adresse IP élastique](#).

Pour modifier le type d'une instance basée sur le stockage d'instances

1. Sauvegardez les données que vous devez conserver, comme suit :
 - Pour les données qui se trouvent sur les volumes de stockage d'instances, sauvegardez-les dans un stockage permanent.
 - Pour les données de vos volumes EBS, créez un instantané des volumes ou détachez le volume de l'instance afin de pouvoir l'attacher ultérieurement à la nouvelle instance.
2. Créez une AMI à partir de votre instance en remplissant les conditions requises et en suivant les procédures décrites dans [Créer une AMI Linux basée sur le stockage d'instance](#). Lorsque vous avez fini de créer un AMI à partir de votre instance, retournez à cette procédure.
3. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
4. Dans le panneau de navigation, sélectionnez AMI. Dans les listes de filtres, choisissez Owned by me (M'appartenant), puis sélectionnez l'image que vous avez créée à l'étape 2. Notez que AMI

name (Nom d'AMI) est le nom que vous avez spécifié quand vous avez enregistré l'image et que Source est votre compartiment Amazon S3.

 Note

Si l'AMI que vous avez créée à l'étape 2 n'apparaît pas, assurez-vous d'avoir sélectionné la région dans laquelle vous avez créé votre AMI.

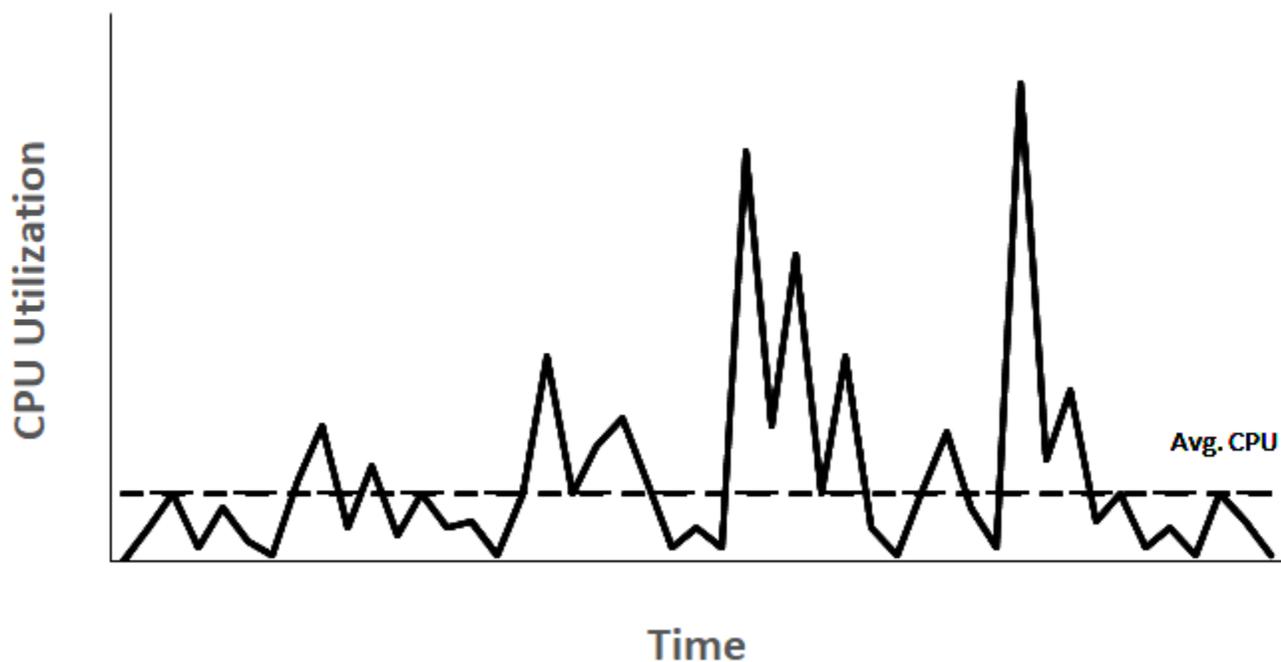
5. Lorsque l'AMI est sélectionnée, choisissez Launch instance from image (Lancer une instance depuis l'image). Lorsque vous configurez l'instance, procédez comme suit :
 - a. Sélectionnez le nouveau type d'instance souhaité. Si le type d'instance que vous souhaitez n'est pas disponible, il n'est pas compatible avec la configuration de l'AMI que vous avez créée. Pour plus d'informations, consultez [Compatibilité pour modifier le type d'instance](#).
 - b. Si vous utilisez une adresse IP élastique, sélectionnez le VPC dans lequel l'instance d'origine s'exécute.
 - c. Si vous voulez autoriser le même trafic pour atteindre la nouvelle instance, sélectionnez le groupe de sécurité associé à l'instance d'origine.
 - d. Une fois que vous avez terminé la configuration de votre nouvelle instance, effectuez les étapes pour sélectionner une paire de clés et lancer votre instance. Il peut s'écouler quelques minutes avant que l'instance ne passe à l'état `running`.
6. Si nécessaire, attachez les nouveaux volumes EBS en fonction des instantanés que vous avez créés, ou les volumes EBS que vous avez détachés de l'instance d'origine, à la nouvelle instance.
7. Installez votre application et les logiciels requis sur la nouvelle instance.
8. Si vous utilisez une adresse IP élastique, attribuez-la à la nouvelle instance comme suit :
 - a. Dans le volet de navigation, sélectionnez Elastic IPs (Adresses IP Elastic).
 - b. Sélectionnez l'adresse IP Elastic associée à l'instance d'origine, choisissez Actions, puis Dissocier l'adresse IP Elastic. Sélectionnez Dissocier lorsque vous êtes invité à confirmer l'opération.
 - c. L'adresse IP Elastic étant toujours sélectionnée, choisissez Actions, puis Associer l'adresse IP Elastic.
 - d. Pour Resource type (Type de ressource), choisissez Instance.
 - e. Pour Instance, choisissez la nouvelle instance à laquelle vous souhaitez associer l'adresse IP élastique.

- f. (Facultatif) Pour Private IP address (Adresse IP privée), spécifiez une adresse IP privée à laquelle associer l'adresse IP Elastic.
 - g. Choisissez Associate.
9. (Facultatif) Vous pouvez terminer l'instance d'origine si elle n'est plus nécessaire. Sélectionnez l'instance, vérifiez que vous êtes sur le point de résilier l'instance d'origine, et non la nouvelle instance (par exemple, vérifiez le nom ou l'heure du lancement), puis sélectionnez Instance state (État de l'instance), Terminate instance (Résilier l'instance).

Instance de performance à capacité extensible

De nombreuses charges de travail polyvalentes ne sont en moyenne pas occupées et ne nécessitent pas un niveau élevé de performances soutenues de l'UC. Le graphique suivant illustre l'utilisation du processeur pour de nombreuses charges de travail courantes que les clients exécutent aujourd'hui dans le AWS cloud.

Many common workloads look like this



Ces charges de travail liées à l'utilisation du low-to-moderate processeur entraînent une perte de cycles du processeur et, par conséquent, vous payez plus que ce que vous utilisez. Pour surmonter ce problème, vous pouvez tirer parti des instances polyvalentes extensibles économiques que sont les instances T.

La famille d'instances T offre les performances d'une UC de base avec la possibilité d'aller au-delà à tout moment et aussi longtemps que nécessaire. L'UC de base est définie pour répondre aux besoins de la majorité des charges de travail polyvalentes, dont les microservices à grande échelle, les serveurs web, les bases de données de petite et moyenne taille, la journalisation des données, les référentiels de code, les bureaux virtuels, les environnements de développement et de test, et les applications stratégiques. Les instances T offrent un équilibre entre les ressources de calcul, de mémoire et de réseau, et constituent le moyen le plus rentable d'exécuter un large éventail d'applications générales nécessitant une utilisation low-to-moderate du processeur. Elles peuvent vous faire économiser jusqu'à 15 % de coûts par rapport à des instances M, voire davantage avec des instances de plus petite taille et plus économiques, dotées de seulement 2 vCPU et 0,5 Gio de mémoire. Les instances T de plus petite taille, telles que nano, micro, small et medium, conviennent parfaitement pour des charges de travail nécessitant une petite quantité de mémoire, non destinées à une utilisation élevée de l'UC.

Note

Cette rubrique décrit le processeur extensible. Pour plus d'informations sur les performances réseau extensibles, consultez [Bande passante réseau d'instance Amazon EC2](#).

Types d'instances extensibles EC2

Les instances extensibles EC2 englobent des types d'instances T4g, T3a et T3, ainsi que T2 de la génération précédente.

Les types d'instances T4g sont la dernière génération d'instances extensibles. Elles offrent le meilleur rapport prix/performance, avec le coût le plus bas de tous les types d'instances EC2. Les types d'instances T4g sont alimentés par des processeurs [AWS Graviton2](#) basés sur ARM bénéficiant d'une prise en charge complète de l'écosystème par des fournisseurs de systèmes d'exploitation, des fournisseurs de logiciels indépendants et des services et applications populaires AWS .

Le tableau suivant récapitule les principales différences entre les types d'instances extensibles.

Type	Description	Famille de processeurs
Dernière génération		
T4g	Type d'instance EC2 le moins cher avec un rapport prix/perf	AWS Processeurs Graviton2 avec cœurs Arm Neoverse N1

Type	Description	Famille de processeurs
	performances jusqu'à 40 % plus élevé et des coûts inférieurs de 20 % par rapport au type d'instance T3	
T3a	instances basées sur x86 les moins coûteuses à des coûts inférieurs de 10 % par rapport à des instances T3	Processeurs AMD EPYC de 1ère génération
T3	Meilleur rapport prix/performances maximales pour les charges de travail x86, jusqu'à 30 % inférieur à celui d'instances T2 de génération précédente	Intel Xeon Scalable (processeurs Skylake, Cascade Lake)
Génération précédente		
T2	instances extensibles de génération précédente	Processeurs Intel Xeon

Pour plus d'informations sur la tarification des instances et des spécifications supplémentaires, consultez [Tarification Amazon EC2](#) et [Types d'instances Amazon EC2](#). Pour plus d'informations sur les performances réseau extensibles, consultez [Bande passante réseau d'instance Amazon EC2](#).

Si votre compte a moins de 12 mois, vous pouvez utiliser une instance `t2.micro` gratuitement (ou une instance `t3.micro` dans les régions où `t2.micro` n'est pas disponible) dans certaines limites d'utilisation. Pour plus d'informations, consultez la page sur l'[AWS offre gratuite](#).

Options d'achat prises en charge pour les instances T

- On-Demand instances
- Reserved instances
- instances dédiées (T3 uniquement)
- Hôtes dédiés (T3 uniquement, uniquement dans le mode standard)

- [Spot instances](#)

Pour plus d'informations, consultez [Options d'achat d'instance](#).

Sommaire

- [Bonnes pratiques](#)
- [Concepts et définitions clés pour les instances de performance à capacité extensible](#)
- [Mode illimité pour les instances de performance à capacité extensible](#)
- [Mode standard pour les instances de performance à capacité extensible](#)
- [Utiliser des instance de performance à capacité extensible](#)
- [Surveiller vos crédits UC pour détecter les instances de performance à capacité extensible](#)

Bonnes pratiques

Suivez ces bonnes pratiques pour tirer le meilleur profit et la plus grande satisfaction des instances de performance à capacité extensible

- Assurez-vous que la taille d'instance que vous choisissez correspond à la configuration minimum requise en matière de mémoire par votre système d'exploitation et vos applications. Les systèmes d'exploitation aux interfaces utilisateur graphiques qui consomment une quantité importante de mémoire et de ressources UC (par exemple Windows) peuvent nécessiter une taille d'instance `t3.micro` ou supérieure dans de nombreux cas d'utilisation. Si les exigences de votre charge de travail en termes de mémoire et d'UC augmentent au fil du temps, les instances T vous offrent la flexibilité nécessaire pour opérer une mise à l'échelle vers des instances de plus grande taille du même type ou d'un autre type.
- Activez [AWS Compute Optimizer](#) pour votre compte, et consultez les recommandations de Compute Optimizer pour votre charge de travail. Compute Optimizer peut vous aider à évaluer l'opportunité d'augmenter la taille des instances pour améliorer les performances, ou de la diminuer pour réduire les coûts. Compute Optimizer peut également recommander un type d'instance différent en fonction de votre scénario. Pour plus d'informations, consultez [Affichage des recommandations d'instances EC2](#) (français non garanti) dans le Guide de l'utilisateur AWS Compute Optimizer .

Concepts et définitions clés pour les instances de performance à capacité extensible

Les types d'instances Amazon EC2 traditionnelles offrent des ressources d'UC fixes, tandis que les instances de performance à capacité extensible fournissent un niveau d'utilisation de l'UC de base avec la possibilité d'atteindre un niveau supérieur. Cela vous garantit de ne payer que pour l'UC de base, plus toute utilisation supplémentaire de l'UC en mode rafale, ce qui entraîne des coûts de calcul réduits. L'utilisation de référence et la possibilité d'extension sont régies par les crédits UC. Les instances de performance à capacité extensible constituent les seuls types d'instances qui utilisent des crédits pour l'utilisation de l'UC.

Chaque instance de performance à capacité extensible gagne des crédits quand son utilisation reste en dessous de la ligne de référence du processeur, et en dépense quand elle la dépasse. Le montant des crédits gagnés et dépensés dépend de l'utilisation de l'UC par l'instance :

- Si l'utilisation de l'UC est inférieure à la ligne de référence, les crédits gagnés sont supérieurs aux crédits dépensés.
- Si l'utilisation de l'UC est égale à la ligne de référence, les crédits gagnés sont égaux aux crédits dépensés.
- Si l'utilisation de l'UC est supérieure à la ligne de référence, les crédits gagnés sont inférieurs aux crédits dépensés.

Quand les crédits gagnés sont supérieurs aux crédits dépensés, la différence est appelée crédits accumulés. Ceux-ci peuvent être utilisés ultérieurement pour dépasser l'utilisation de référence de l'UC. De même, quand les crédits dépensés sont supérieurs aux crédits gagnés, le comportement de l'instance dépend selon que le crédit est configuré en mode Standard ou Illimité.

En mode Standard, quand les crédits dépensés sont supérieurs aux crédits gagnés, l'instance utilise les crédits accumulés pour dépasser l'utilisation de référence de l'UC. S'il ne reste pas de crédits accumulés, l'instance revient progressivement à l'utilisation de référence de l'UC, sans plus pouvoir dépasser la ligne de référence tant qu'elle n'a pas accumulé davantage de crédits.

En mode Illimité, si l'instance dépasse l'utilisation de référence de l'UC, elle commence par utiliser les crédits accumulés. S'il n'en reste pas, l'instance dépense des crédits excédentaires. Si son utilisation de l'UC chute au-dessous du niveau de référence, elle se sert des crédits UC gagnés pour rembourser progressivement les crédits excédentaires dépensés plus tôt. La possibilité de gagner des crédits UC pour rembourser progressivement des crédits excédentaires permet à Amazon EC2 d'obtenir l'utilisation moyenne de l'UC d'une instance sur une période de 24 heures.

Si l'utilisation moyenne du CPU dépasse le niveau de base pendant une période de 24 heures, l'utilisation supplémentaire est facturée pour l'instance selon un [tarif supplémentaire fixe](#) par heure de vCPU.

Table des matières

- [Concepts clés et définitions](#)
- [Gagner des crédits UC](#)
- [Taux d'obtention de crédits UC](#)
- [Limite d'accumulation de crédits UC](#)
- [Durée de vie des crédits UC accumulés](#)
- [Utilisation de référence](#)

Concepts clés et définitions

Les concepts clés et définitions qui suivent s'appliquent aux instances de performance à capacité extensible.

Utilisation de l'UC

L'utilisation de l'UC est le pourcentage d'unités de calcul EC2 allouées actuellement utilisées sur l'instance. Cette métrique mesure le pourcentage de cycles d'UC alloués qui sont utilisés sur une instance. La CloudWatch métrique d'utilisation du processeur indique l'utilisation du processeur par instance et non l'utilisation du processeur par cœur. La spécification d'UC de base d'une instance est également basée sur l'utilisation de l'UC par instance. Pour mesurer l'utilisation du processeur à l'aide de l'AWS Management Console ou de l'AWS CLI, voir [Obtenir les statistiques d'une instance spécifique](#).

Crédits d'UC

Unité de temps de vCPU.

Exemples :

1 crédit d'UC = 1 vCPU * 100 % d'utilisation * 1 minute.

1 crédit d'UC = 1 vCPU * 50 % d'utilisation * 2 minutes.

1 crédit d'UC = 2 vCPU * 25 % d'utilisation * 2 minutes

Utilisation de référence

L'utilisation de référence est le niveau auquel le CPU peut être utilisé pour un solde créditeur net de zéro, lorsque le nombre de crédits CPU gagnés correspond au nombre de crédits CPU utilisés. L'utilisation de référence est également appelée la référence. L'utilisation de référence est exprimée en pourcentage de l'utilisation du vCPU, calculé comme suit : % d'utilisation de référence = (nombre de crédits gagnés/nombre de vCPU)/60 minutes.

Pour connaître l'utilisation de référence de chaque type d'instance à capacité extensible, consultez le [tableau des crédits](#).

Crédits gagnés

Crédits gagnés par une instance pendant son exécution.

Nombre de crédits gagnés par heure = % d'utilisation de référence * nombre de vCPU * 60 minutes

Exemple :

Un t3.nano avec 2 vCPU et une utilisation de référence de 5 % gagne 6 crédits par heure, calculés comme suit :

$2 \text{ vCPU} * 5 \% \text{ de référence} * 60 \text{ minutes} = 6 \text{ crédits par heure}$

Crédits dépensés ou utilisés

Crédits utilisés par une instance pendant son exécution.

Crédits d'UC dépensés par minute = nombre de vCPU * utilisation de l'UC * 1 minute

Crédits accumulés

Crédits d'UC non dépensés quand une instance utilise moins de crédits que ce que requiert l'utilisation de référence. En d'autres termes, les crédits accumulés = (crédits gagnés - crédits utilisés) inférieurs à la base de référence.

Exemple :

Si un t3.nano s'exécute à 2 % d'utilisation de l'UC, ce qui est inférieur à sa ligne de référence de 5 %, pendant une heure, les crédits accumulés sont calculés comme suit :

Crédits d'UC accumulés = (crédits gagnés par heure - crédits utilisés par heure) = $6 - 2 \text{ vCPU} * 2 \% \text{ d'utilisation de l'UC} * 60 \text{ minutes} = 6 - 2,4 = 3,6 \text{ crédits accumulés par heure}$

Limite d'accumulation de crédit

Dépend de la taille de l'instance mais, en général, est égale au nombre maximum de crédits gagnés en 24 heures.

Exemple :

Pour t3.nano, la limite d'accumulation de crédit = $24 * 6 = 144$ crédits

Crédits de lancement

Applicables uniquement pour des instances T2 configurées pour le mode Standard. Les crédits de lancement sont un nombre limité de crédits d'UC qui sont alloués à une nouvelle instance T2 afin que, une fois lancée en mode Standard, elle puisse dépasser la ligne de référence.

Crédits excédentaires

Crédits dépensés par une instance après qu'elle a épuisé son solde de crédits accumulés. Les crédits excédentaires sont conçus pour permettre à des instances extensibles de soutenir des performances élevées pendant une période prolongée, et ne sont utilisés qu'en mode Illimité. Le solde de crédits excédentaires est utilisé pour déterminer combien de crédits l'instance a utilisés pour dépasser la ligne de référence en mode Illimité.

Mode Standard

Mode de configuration du crédit permettant à une instance de dépasser sa ligne de référence en dépensant les crédits accumulés dans son solde de crédit.

Mode Illimité

Mode de configuration du crédit permettant à une instance de dépasser sa ligne de référence en soutenant une utilisation élevée de l'UC pendant une période quelconque en cas de nécessité. Le prix horaire d'une instance couvre automatiquement tous les pics d'utilisation d'UC si l'utilisation moyenne de l'UC de l'instance est égale ou inférieure au niveau de base sur une période glissante de 24 heures ou pendant la durée de vie de l'instance si celle-ci est plus courte. Si l'instance s'exécute avec une utilisation de l'UC supérieure pendant une période prolongée, c'est possible moyennant des [frais supplémentaires fixes](#) par heure vCPU.

Le tableau suivant récapitule les principales différences de crédit entre les types d'instances extensibles.

Type	Type de crédits d'UC pris en charge	Modes de configuration du crédit	Durée de vie des crédits d'UC accumulés entre les démarrages et les arrêts d'instance
Dernière génération			
T4g	Crédits gagnés, Crédits accumulés, Crédits dépensés, Crédits excédentaires (mode illimité uniquement)	Standard, Illimité (par défaut)	7 jours (les crédits persistent pendant 7 jours après l'arrêt d'une instance)
T3a	Crédits gagnés, Crédits accumulés, Crédits dépensés, Crédits excédentaires (mode illimité uniquement)	Standard, Illimité (par défaut)	7 jours (les crédits persistent pendant 7 jours après l'arrêt d'une instance)
T3	Crédits gagnés, Crédits accumulés, Crédits dépensés, Crédits excédentaires (mode illimité uniquement)	Standard, Illimité (par défaut)	7 jours (les crédits persistent pendant 7 jours après l'arrêt d'une instance)
Génération précédente			
T2	Crédits gagnés, Crédits accumulés, Crédits dépensés, Crédits de lancement (mode Standard uniquement), Crédits	Standard (par défaut), Illimité	0 jour (les crédits sont perdus quand une instance s'arrête)

Type	Type de crédits d'UC pris en charge	Modes de configuration du crédit	Durée de vie des crédits d'UC accumulés entre les démarrages et les arrêts d'instance
	excédentaires (mode illimité uniquement)		

Note

Le mode illimité n'est pas pris en charge pour les instances T3 lancées sur un hôte dédié.

Gagner des crédits UC

Chaque instance de performance à capacité extensible gagne continuellement (à une résolution de l'ordre de la milliseconde) un taux déterminé de crédits UC par heure, en fonction de sa taille. Le processus de comptabilité par lequel les crédits s'accumulent ou sont dépensés se fait également sur une résolution de l'ordre de la milliseconde. Vous n'avez donc pas à vous soucier de consommer trop de crédits UC ; une brève rafale dans l'utilisation de l'UC ne se sert que d'une petite quantité des crédits UC.

Si une instance de performance à capacité extensible utilise moins de ressources d'UC que ne le requière son utilisation de référence (par exemple lorsqu'elle est inactive), les crédits UC inutilisés sont accumulés dans le solde de crédits UC. Si une instance de performance à capacité extensible a besoin d'étendre l'utilisation au-dessus du niveau d'utilisation de référence, elle dépense les crédits accumulés. Plus une instance de performance à capacité extensible accumule de crédits, plus elle peut dépasser son niveau d'utilisation de référence longtemps, quand l'UC le demande.

Le tableau ci-dessous répertorie les types d'instances à performances extensibles, le taux auquel les crédits UC sont gagnés par heure, le nombre maximal de crédits UC gagnés qu'une instance peut accumuler, le nombre de processeurs vCPU par instance et le niveau d'utilisation de référence sous la forme d'un pourcentage des performances d'un cœur complet (utilisant un seul processeur vCPU).

Type d'instance	Crédits UC gagnés par heure	Maximum de crédits gagnés pouvant être accumulés*	vCPU***	Utilisation de référence par vCPU
T2				
t2.nano	3	72	1	5 %
t2.micro	6	144	1	10 %
t2.small	12	288	1	20 %
t2.medium	24	576	2	20%**
t2.large	36	864	2	30%**
t2.xlarge	54	1296	4	22,5%**
t2.2xlarge	81.6	1958.4	8	17%**
T3				
t3.nano	6	144	2	5%**
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
T3a				
t3a.nano	6	144	2	5%**
t3a.micro	12	288	2	10%**

Type d'instance	Crédits UC gagnés par heure	Maximum de crédits gagnés pouvant être accumulés*	vCPU***	Utilisation de référence par vCPU
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**
T4g				
t4g.nano	6	144	2	5%**
t4g.micro	12	288	2	10%**
t4g.small	24	576	2	20%**
t4g.medium	24	576	2	20%**
t4g.large	36	864	2	30%**
t4g.xlarge	96	2304	4	40%**
t4g.2xlarge	192	4608	8	40%**

* Le nombre de crédits pouvant être accumulés est équivalent au nombre de crédits pouvant être gagnés en 24 heures.

** Le pourcentage d'utilisation de référence dans le tableau est par vCPU. Dans CloudWatch, l'utilisation du processeur est affichée par vCPU. Par exemple, l'utilisation du processeur pour une t3.large instance fonctionnant au niveau de référence est indiquée comme 30 % dans les

métriques CloudWatch du processeur. Pour plus d'informations sur le calcul de l'utilisation de référence, consultez [Utilisation de référence](#).

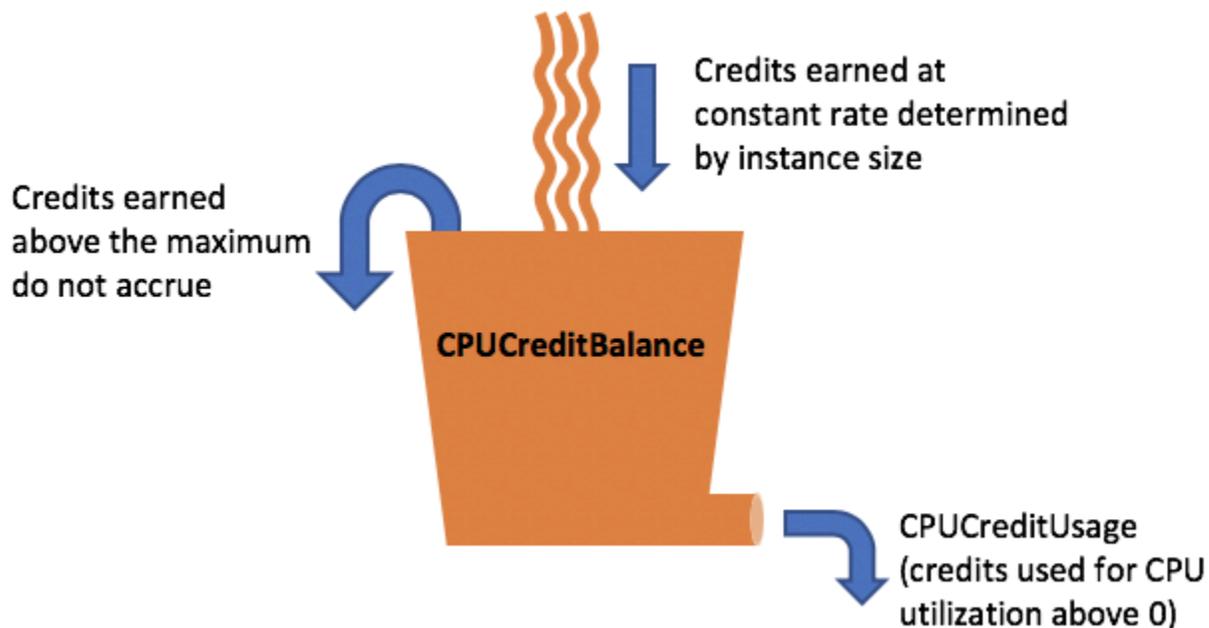
*** Chaque vCPU est un thread d'un cœur Intel Xeon ou AMD EPYC, à l'exception des instances T2 et T4g.

Taux d'obtention de crédits UC

Le nombre de crédits UC gagnés par heure est déterminé par la taille d'instance. Par exemple, une instance `t3.nano` gagne six crédits par heure, tandis qu'une instance `t3.small` en gagne 24 par heure. Le tableau précédent répertorie le taux d'obtention de crédits pour l'ensemble des instances.

Limite d'accumulation de crédits UC

Si les crédits gagnés n'expirent jamais sur une instance en cours d'exécution, il existe une limite pour le nombre de crédits gagnés pouvant être accumulés par une instance. Cette limite est déterminée par la limite du solde de crédits UC. Une fois la limite atteinte, les nouveaux crédits gagnés sont rejetés, comme l'indique l'image suivante. Le compartiment plein indique la limite du solde de crédits UC, tandis que le débordement signale les crédits excédant la limite qui viennent d'être gagnés.



La limite du solde de crédits UC diffère pour chaque taille d'instance. Par exemple, une instance `t3.micro` peut accumuler un maximum de 288 crédits UC gagnés dans le solde de crédits UC.

Le tableau précédent répertorie le nombre maximum de crédits gagnés pouvant être cumulés par instance

Les instances T2 standard gagnent également des crédits de lancement. Les crédits de lancement ne sont pas comptés dans la limite du solde de crédits UC. Si une instance T2 n'a pas dépensé ses crédits de lancement et reste inactive pendant 24 heures tout en accumulant des crédits gagnés, son solde de crédits d'UC est affiché comme dépassant la limite. Pour plus d'informations, consultez [Crédits de lancement](#).

Les instances T4g, T3a et T3 instances ne gagnent pas de crédits de lancement. Ces instances sont lancées en mode `unlimited` par défaut et peuvent par conséquent s'exécuter en mode rafale immédiatement après leur démarrage, sans avoir besoin de crédits de lancement. Les instances T3 lancées sur un lancement d'hôte dédié `standardby default ;unlimited` (par défaut) ne sont pas prises en charge sur un Hôte Dédié pour les instances T3.

Durée de vie des crédits UC accumulés

Les crédits UC sur une instance en cours d'exécution n'expirent pas.

Pour T2, le solde de crédits UC n'est pas conservé entre les arrêts et les démarrages des instances. Si vous arrêtez une instance T2, celle-ci perd tous ses crédits accumulés.

Pour les instances T4g, T3a et T3, le solde de crédits d'UC est conservé pendant sept jours après l'arrêt d'une instance. Ensuite, les crédits sont perdus. Si vous démarrez l'instance dans les sept jours, aucun crédit n'est perdu.

Pour plus d'informations, consultez `CPUCreditBalance` le [tableau CloudWatch des mesures](#).

Utilisation de référence

L'utilisation de référence est le niveau auquel le CPU peut être utilisé pour un solde créditeur net de zéro, lorsque le nombre de crédits CPU gagnés correspond au nombre de crédits CPU utilisés. L'utilisation de référence est également appelée la référence.

L'utilisation de référence est exprimée en pourcentage de l'utilisation du vCPU, calculé comme suit :

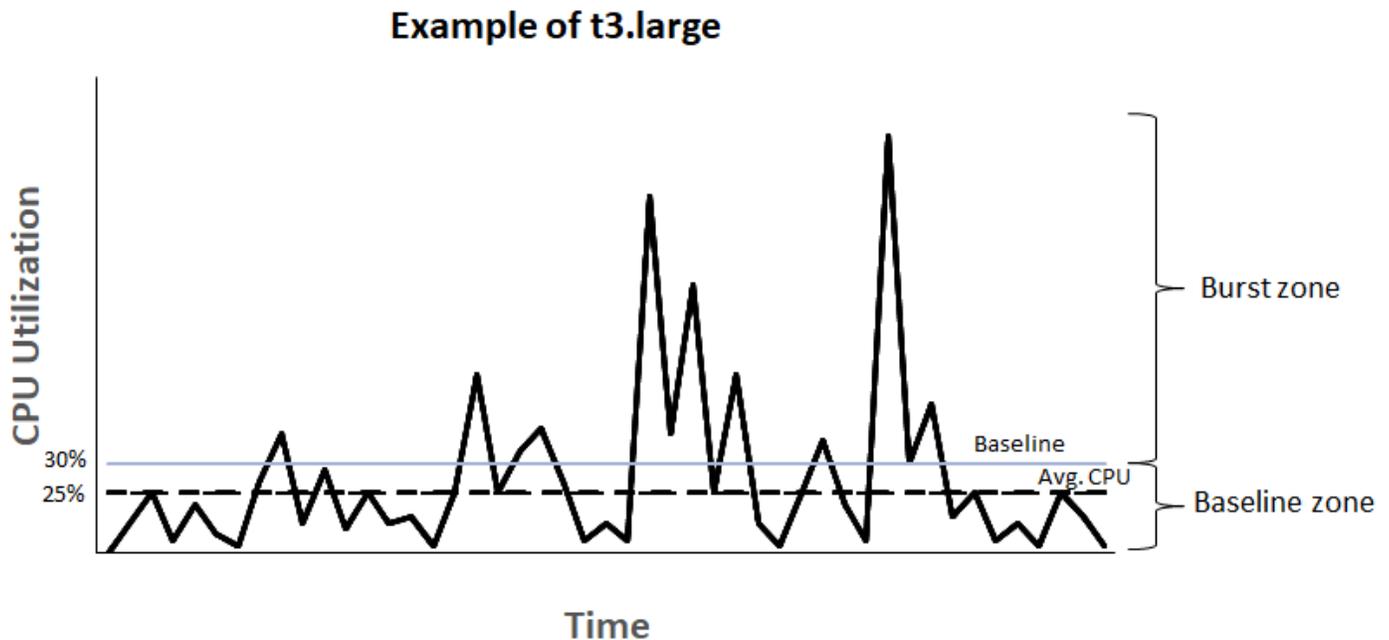
$$\text{(number of credits earned/number of vCPUs)/60 minutes} = \% \text{ baseline utilization}$$

Par exemple, une instance `t3.nano`, avec 2 vCPU, gagne 6 crédits par heure, ce qui donne une utilisation de référence de 5 %, calculée comme suit :

$(6 \text{ credits earned} / 2 \text{ vCPUs}) / 60 \text{ minutes} = 5\% \text{ baseline utilization}$

Une `t3.large` instance dotée de 2 vCPU génère 36 crédits par heure, soit une utilisation de base de 30 % ($(36/2)/60$).

Le graphique suivant fournit un exemple d'utilisation moyenne du processeur inférieure à la ligne de base. `t3.large`



Mode illimité pour les instances de performance à capacité extensible

Une instance de performance à capacité extensible configurée en mode `unlimited` peut maintenir une utilisation d'UC élevée pour toute période donnée en cas de nécessité. Le prix horaire d'une instance couvre automatiquement tous les pics d'utilisation d'UC si l'utilisation moyenne de l'UC de l'instance est égale ou inférieure au niveau de base sur une période glissante de 24 heures ou pendant la durée de vie de l'instance si celle-ci est plus courte.

Pour la majorité des charges de travail à usage général, les instances configurées en mode `unlimited` fournissent d'excellentes performances sans frais supplémentaires. Si l'instance s'exécute avec une utilisation d'UC supérieure pendant une période prolongée, c'est possible moyennant des frais supplémentaires fixes par heure vCPU. Pour en savoir plus sur la tarification, consultez [Tarification Amazon EC2](#) et [Tarification des instances T2/T3/T4 en mode illimité](#).

Si vous utilisez une instance `t2.micro` ou `t3.micro` relevant de [AWS l'offre gratuite](#) et si vous l'utilisez en mode `unlimited`, des frais peuvent s'appliquer si votre utilisation moyenne sur une période glissante de 24 heures excède [l'utilisation de référence](#) de l'instance.

Les instances T4g, T3a et T3 sont lancées `unlimited` par défaut (sauf si vous [modifiez la](#) valeur par défaut). Si l'utilisation moyenne de l'UC sur une période de 24 heures dépasse le niveau de référence, vous devrez payer des frais pour les crédits excédentaires. Si vous lancez des instances Spot en mode `unlimited` et que vous prévoyez de les utiliser immédiatement et pour une courte durée, sans temps d'inactivité pour accumuler les crédits d'UC, vous devrez payer des frais pour les crédits excédentaires. Nous vous recommandons de lancer vos instances Spot en mode [standard](#) pour éviter des coûts plus élevés. Pour plus d'informations, consultez [Les crédits excédentaires peuvent occasionner des frais](#) et [Instances de performance à capacité extensible](#).

Note

Les instances T3 lancées sur un lancement d'hôte dédié `standardby default ;unlimited` (par défaut) ne sont pas prises en charge sur un Hôte Dédié pour les instances T3.

Table des matières

- [Concepts du mode illimité \(Unlimited\)](#)
 - [Fonctionnement des instances de performance à capacité extensible illimitées](#)
 - [Quand utiliser le mode illimité/mode d'UC fixe ?](#)
 - [Les crédits excédentaires peuvent occasionner des frais](#)
 - [Pas de crédit de lancement pour les instances T2 illimitées](#)
 - [Activer le mode illimité](#)
 - [Comportement des crédits lors du basculement entre Illimité et Standard](#)
 - [Surveiller l'utilisation du crédit](#)
- [Exemples de modes illimités](#)
 - [Exemple 1 : Expliquer l'utilisation des crédits avec T3 illimité](#)
 - [Exemple 2 : Expliquer l'utilisation des crédits avec T2 illimité](#)

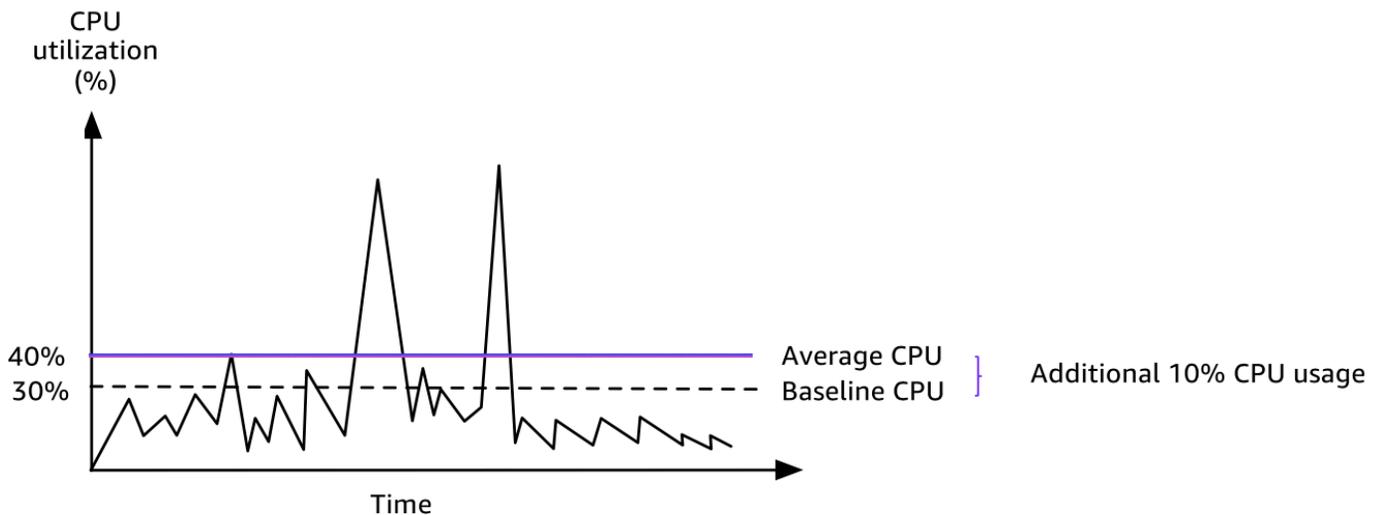
Concepts du mode illimité (Unlimited)

Le mode `unlimited` est une option de configuration de crédit pour les instances de performance à capacité extensible. Il peut être activé ou désactivé à tout moment pour une instance en cours d'exécution ou arrêtée. Vous pouvez [la définir `unlimited` comme option de crédit par défaut](#) au niveau du compte, par AWS région, par famille d'instances de performance éclatante, afin que toutes les nouvelles instances de performance actualisées du compte soient lancées à l'aide de l'option de crédit par défaut.

Fonctionnement des instances de performance à capacité extensible illimitées

Si une instance de performance à capacité extensible configurée en mode `unlimited` épuise son solde de crédits UC, elle peut dépenser ses crédits excédentaires pour dépasser le [niveau de référence](#). Si son utilisation de l'UC chute au-dessous du niveau de référence, elle se sert des crédits UC gagnés pour rembourser progressivement les crédits excédentaires dépensés plus tôt. La possibilité de gagner des crédits UC pour rembourser progressivement des crédits excédentaires permet à Amazon EC2 d'obtenir l'utilisation moyenne de l'UC d'une instance sur une période de 24 heures. Si l'utilisation moyenne du CPU dépasse le niveau de base pendant une période de 24 heures, l'utilisation supplémentaire est facturée pour l'instance selon un [tarif supplémentaire fixe](#) par heure de vCPU.

Le graphique suivant montre l'utilisation de l'UC d'une instance `t3.large`. Le niveau de base de l'utilisation de l'UC pour une instance `t3.large` est de 30 %. Si l'instance s'exécute à un taux d'utilisation d'UC de 30 % ou moins en moyenne sur une période de 24 heures, aucun frais supplémentaire ne s'applique, car le coût est déjà couvert par le prix horaire de l'instance. Toutefois, si l'instance s'exécute à un taux d'utilisation de CPU de 40 % en moyenne sur une période de 24 heures, comme le montre le graphique, les 10 % supplémentaires d'utilisation du CPU sont facturés pour l'instance selon un [tarif supplémentaire fixe](#) par heure de vCPU.



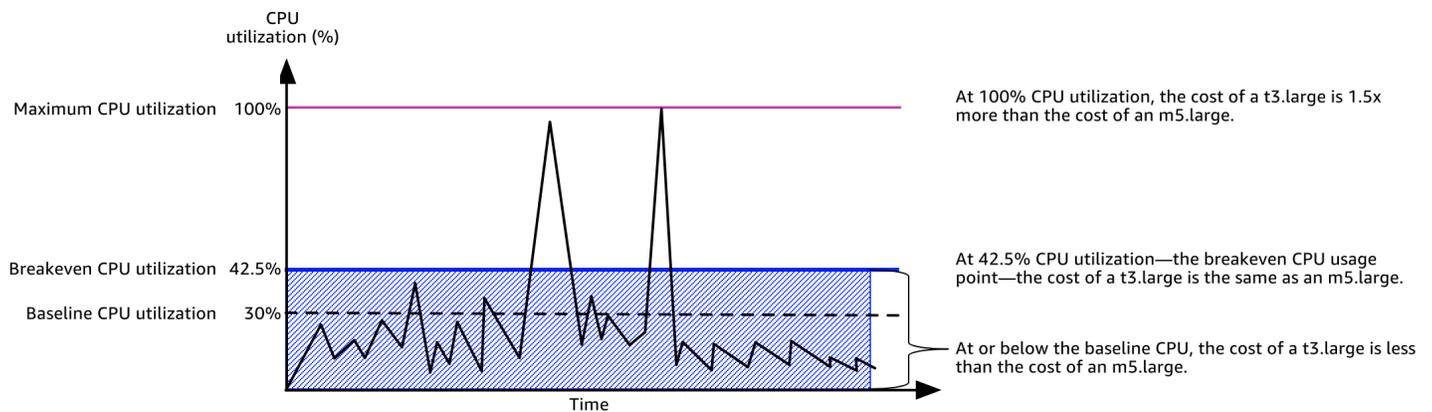
Pour plus d'informations sur l'utilisation de référence par vCPU pour chaque type d'instance et sur le nombre de crédits gagnés par chaque type d'instance, consultez le [tableau des crédits](#).

Quand utiliser le mode illimité/mode d'UC fixe ?

Pour déterminer si vous devez utiliser une instance de performance à capacité extensible en mode `unlimited`, telle qu'une instance T3, ou une instance à performance fixe, telle qu'une instance M5, vous devez déterminer l'utilisation d'UC de seuil de rentabilité. L'utilisation d'UC de seuil de rentabilité pour une instance de performance à capacité extensible de performance à capacité extensible est le point où une instance de performance à capacité extensible coûte autant qu'une instance à performance fixe. L'utilisation d'UC de seuil de rentabilité vous aide à déterminer les éléments suivants :

- Si l'utilisation moyenne de l'UC sur une période de 24 heures est égale ou inférieure à l'utilisation d'UC de seuil de rentabilité, utilisez une instance de performance à capacité extensible en mode `unlimited` afin de pouvoir bénéficier du prix inférieur d'une instance de performance à capacité extensible tout en profitant de la même performance que fournirait une instance à performance fixe.
- Si l'utilisation moyenne de l'UC sur une période de 24 heures est supérieure à l'utilisation d'UC de seuil de rentabilité, l'instance de performance à capacité extensible coûtera plus qu'une instance à performance fixe de taille équivalente. Si une instance T3 fonctionne continuellement à un taux d'utilisation d'UC de 100 %, vous paierez en définitive environ 1,5 fois le prix d'une instance M5 de taille équivalente.

Le graphique suivant montre l'utilisation d'UC de seuil de rentabilité où une instance `t3.large` coûte autant qu'une instance `m5.large`. L'utilisation d'UC de seuil de rentabilité pour une instance `t3.large` est de 42,5 %. Si l'utilisation moyenne de l'UC est de 42,5 %, le coût de l'exécution de l'instance `t3.large` est identique à celui d'une instance `m5.large`, et il s'avère supérieur si l'utilisation moyenne de l'UC dépasse 42,5 %. Si la charge de travail nécessite une utilisation moyenne de l'UC inférieure à 42,5 %, vous pouvez tirer profit du prix inférieur de l'instance `t3.large` tout en obtenant la même performance que fournirait une instance `m5.large`.



Le tableau suivant indique comment calculer l'utilisation d'UC de seuil de rentabilité, qui vous permettra de déterminer quand il est moins onéreux d'utiliser une instance de performance à capacité extensible en mode `unlimited` ou une instance à performance fixe. Les colonnes du tableau sont étiquetées de A à K.

Type d'instance	vCPU	T3 – Prix*/heure	M5 – Prix*/heure	Différence de prix	Utilisation de référence par vCPU (%)	Frais par heure de processeur virtuel pour crédits excédentaires	Frais par minute de processeur virtuel	Minutes d'extension supplémentaires disponibles par processeur virtuel	% d'UC supplémentaire disponible	% d'UC de seuil de rentabilité
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	0,0835 USD	0,096 USD	0,0125 USD	30 %	0,05 USD	0,000833 USD	15	12,5%	42,5 %

* Le prix se rapporte à la région us-east-1 et au système d'exploitation Linux.

Le tableau fournit les informations suivantes :

- La colonne A indique le type d'instance, t3.large.
- La colonne B indique le nombre de processeurs virtuels pour l'instance t3.large.
- La colonne C indique le prix d'une instance t3.large par heure.
- La colonne D indique le prix d'une instance m5.large par heure.
- La colonne E indique la différence de prix entre l'instance t3.large et l'instance m5.large.
- La colonne F indique l'utilisation de référence par vCPU de l'instance t3.large, qui est de 30 %. Au niveau de base, le coût horaire de l'instance couvre le coût de l'utilisation de l'UC.
- La colonne G indique les [frais supplémentaires fixes](#) par heure de vCPU facturés pour une instance si elle passe à 100 % d'utilisation de CPU après avoir épuisé ses crédits gagnés.
- La colonne H indique les [frais supplémentaires fixes](#) par minute de vCPU facturés pour une instance si elle passe à 100 % d'utilisation de CPU après avoir épuisé ses crédits gagnés.

- La colonne I indique le nombre de minutes supplémentaires pendant lesquelles l'instance `t3.large` peut fonctionner par heure à 100 % d'UC pour le même prix par heure qu'une instance `m5.large`.
- La colonne J indique l'utilisation d'UC supplémentaire (en %) par rapport à l'utilisation de base que l'instance peut assurer pour le même prix par heure qu'une instance `m5.large`.
- La colonne K indique l'utilisation d'UC de seuil de rentabilité (en %) que l'instance `t3.large` peut assurer sans générer plus de frais que l'instance `m5.large`. Au dessus de ce seuil, l'instance `t3.large` coûte plus que l'instance `m5.large`.

Le tableau ci-dessous indique l'utilisation d'UC de seuil de rentabilité (en %) des types d'instance T3 par rapport aux types d'instance M5 de taille équivalente.

Type d'instance T3	Utilisation d'UC de seuil de rentabilité (en %) de T3 par rapport à M5
<code>t3.large</code>	42,5 %
<code>t3.xlarge</code>	52,5 %
<code>t3.2xlarge</code>	52,5 %

Les crédits excédentaires peuvent occasionner des frais

Si l'utilisation moyenne de l'UC d'une instance est égale ou inférieure au niveau de base, aucuns frais supplémentaires ne sont appliqués à l'instance. Comme une instance gagne un [nombre maximum de crédits](#) sur une période de 24 heures (par exemple, une instance `t3.micro` peut acquérir un maximum de 288 crédits sur une période de 24 heures), elle peut dépenser des crédits excédentaires jusqu'à ce maximum sans être facturée immédiatement.

Cependant, si l'utilisation de l'UC reste supérieure au niveau de référence, l'instance ne peut pas gagner suffisamment de crédits pour rembourser progressivement les crédits excédentaires qu'elle a dépensés. Des frais supplémentaires fixes s'appliquent par heure vCPU aux crédits excédentaires qui ne sont pas remboursés progressivement. Pour en savoir plus sur les frais applicables, consultez [Tarification des instances T2/T3/T4g en mode illimité](#).

Les crédits excédentaires qui ont été dépensés précédemment sont facturés lorsque l'une des situations suivantes se produit :

- Les crédits excédentaires dépensés dépassent le [nombre maximum de crédits](#) que l'instance peut gagner sur une période de 24 heures. Les crédits excédentaires dépensés au-dessus de ce maximum sont facturés à la fin de l'heure.
- L'instance est arrêtée ou résiliée.
- L'instance bascule du mode `unlimited` au mode `standard`.

Les crédits excédentaires dépensés sont suivis par la CloudWatch métrique `CPU Surplus Credit Balance`. Les crédits excédentaires facturés sont suivis selon la CloudWatch métrique `CPU Surplus Credits Charged`. Pour plus d'informations, consultez [CloudWatch Mesures supplémentaires pour les instances de performance éclatantes](#).

Pas de crédit de lancement pour les instances T2 illimitées

Les instances T2 standard reçoivent des [crédits de lancement](#), mais les instances T2 illimité n'en reçoivent pas. Une instance T2 illimité peut dépasser le niveau de référence à tout moment sans frais supplémentaires tant que l'utilisation moyenne de son UC est égale ou inférieure au niveau de référence sur une période glissante de 24 heures ou pendant sa durée de vie (selon la période la plus courte). De ce fait, les instances T2 illimité ne nécessitent pas de crédits de lancement pour obtenir des performances élevées dès le lancement.

Si une instance T2 passe du mode `standard` au mode `unlimited`, tous les crédits de lancement accumulés sont supprimés de la métrique `CPU Credit Balance` avant que la métrique `CPU Credit Balance` restante soit reportée.

Les instances T4g, T3a et T3 ne reçoivent jamais de crédits de lancement parce qu'elles prennent en charge le mode Illimité. La configuration du crédit en mode illimité permet aux instances T4g, T3a et T3 d'utiliser autant d'UC que nécessaire pour dépasser la ligne de référence aussi longtemps que nécessaire.

Activer le mode illimité

Vous pouvez passer du mode `unlimited` au mode `standard` et du mode `standard` au mode `unlimited` à tout moment sur une instance en cours d'exécution ou arrêtée. Pour plus d'informations, consultez [Lancer une instance de performance à capacité extensible en mode Illimité ou Standard](#) et [Modifier la spécification de crédits d'une instance de performance à capacité extensible](#).

Vous pouvez la définir `unlimited` comme option de crédit par défaut au niveau du compte, par AWS région, par famille d'instances de performance éclatante, afin que toutes les nouvelles

instances de performance actualisées du compte soient lancées à l'aide de l'option de crédit par défaut. Pour plus d'informations, consultez [Définir la spécification de crédits par défaut pour le compte](#).

Vous pouvez vérifier si une instance de performance à capacité extensible est configurée en mode `unlimited` ou `standard` à l'aide de la console Amazon EC2 ou de la AWS CLI. Pour plus d'informations, consultez [Afficher la spécification de crédits d'une instance de performance à capacité extensible](#) et [Afficher la spécification de crédits par défaut](#).

Comportement des crédits lors du basculement entre Illimité et Standard

`CPUCreditBalance` est une CloudWatch métrique qui suit le nombre de crédits accumulés par une instance. `CPUSurplusCreditBalance` est une CloudWatch métrique qui suit le nombre de crédits excédentaires dépensés par une instance.

Lorsque vous passez en mode `standard` une instance qui était configurée en mode `unlimited`, voici ce qui se produit :

- La valeur de `CPUCreditBalance` reste inchangée et est reportée.
- La valeur de `CPUSurplusCreditBalance` est immédiatement facturée.

Lorsqu'une instance `standard` passe à la configuration `unlimited`, la situation suivante se produit :

- La valeur de `CPUCreditBalance` contenant les crédits gagnés accumulés est reportée.
- Pour les instances T2 `standard`, tous les crédits de lancement sont supprimés de la valeur de `CPUCreditBalance` et la valeur de `CPUCreditBalance` restante contenant les crédits gagnés accumulés est reportée.

Surveiller l'utilisation du crédit

Pour savoir si votre instance dépense plus de crédits que ce que la base de référence fournit, vous pouvez utiliser CloudWatch des métriques pour suivre l'utilisation, et vous pouvez configurer des alarmes horaires pour être informé de l'utilisation des crédits. Pour plus d'informations, consultez [Surveiller vos crédits UC pour détecter les instances de performance à capacité extensible](#).

Exemples de modes illimités

Les exemples suivants expliquent l'utilisation des crédits lorsque des instances sont configurées en mode `unlimited`.

Exemples

- [Exemple 1 : Expliquer l'utilisation des crédits avec T3 illimité](#)
- [Exemple 2 : Expliquer l'utilisation des crédits avec T2 illimité](#)

Exemple 1 : Expliquer l'utilisation des crédits avec T3 illimité

Cet exemple montre l'utilisation de l'UC d'une instance `t3.nano` lancée en mode `unlimited` et comment l'instance dépense les crédits gagnés et excédentaires pour maintenir l'utilisation de l'UC.

Une instance `t3.nano` gagne 144 crédits UC sur une période glissante de 24 heures, qu'elle peut rembourser pour 144 minutes d'utilisation de processeur vCPU. Lorsqu'il épuise le solde créditeur de son processeur (représenté par la CloudWatch métrique `CPUCreditBalance`), il peut dépenser les crédits CPU excédentaires, qu'il n'a pas encore gagnés, pour augmenter aussi longtemps qu'il en a besoin. Comme une instance `t3.nano` gagne un maximum de 144 crédits sur une période de 24 heures, elle peut dépenser des crédits excédentaires jusqu'à ce maximum sans être facturée immédiatement. Si elle dépense plus de 144 crédits UC, la différence fait l'objet d'une facturation à la fin de l'heure.

L'exemple illustré par le graphique suivant a pour but de montrer comment une instance peut passer en mode rafale à l'aide des crédits excédentaires, même après avoir épuisé son `CPUCreditBalance`. Le flux de travail suivant référence les points numérotés sur le graphique :

P1 – À 0 heure sur le graphe, l'instance est lancée en mode `unlimited` et commence immédiatement à gagner des crédits. L'instance reste inactive après son lancement (l'utilisation de l'UC est de 0 %) et aucun crédit n'est dépensé. Tous les crédits non dépensés sont accumulés dans le solde de crédits. Pendant les premières 24 heures, `CPUCreditUsage` est à 0 et la valeur de `CPUCreditBalance` atteint son maximum de 144.

P2 – Pendant les 12 heures suivantes, l'utilisation de l'UC est à 2,5 %, ce qui est inférieur au niveau de référence de 5 %. L'instance gagne plus de crédits qu'elle n'en dépense, mais la valeur de `CPUCreditBalance` ne peut pas dépasser son maximum de 144 crédits.

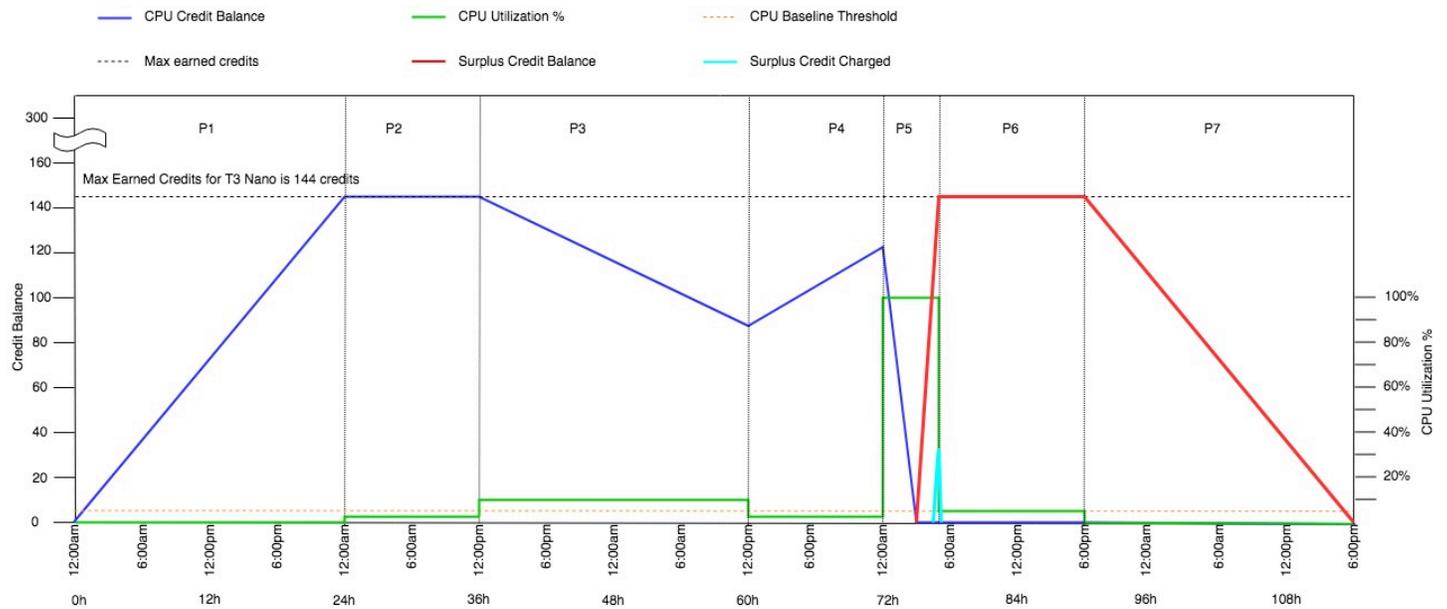
P3 – Pendant les 24 heures suivantes, l'utilisation de l'UC est de 7 % (au-dessus du niveau de référence), ce qui nécessite la dépense de 57,6 crédits. L'instance dépense plus de crédits qu'elle n'en gagne et la valeur de `CPUCreditBalance` baisse jusqu'à 86,4 crédits.

P4 – Pendant les 12 heures suivantes, l'utilisation de l'UC baisse jusqu'à 2,5 % (sous le niveau de référence), ce qui nécessite la dépense de 36 crédits. Au même moment, l'instance gagne 72 crédits. L'instance gagne plus de crédits qu'elle n'en dépense et la valeur `CPUCreditBalance` augmente jusqu'à 122 crédits.

P5 – Pendant les 5 heures suivantes, l'instance est à un pic de 100 % d'utilisation de l'UC et dépense un total de 570 crédits pour maintenir ce pic. Environ une heure après le début de cette période, l'instance épuise son solde `CPUCreditBalance` complet de 122 crédits et commence à dépenser les crédits excédentaires pour maintenir l'utilisation de l'UC élevée, totalisant 448 crédits excédentaires dans cette période ($570-122=448$). Lorsque la valeur de `CPUSurplusCreditBalance` atteint 144 crédits d'UC (maximum qu'une instance `t3.nano` peut gagner dans une période de 24 heures), les crédits excédentaires dépensés par la suite ne peuvent pas être compensés par les crédits gagnés. Les crédits excédentaires dépensés par la suite s'élèvent à 304 crédits ($448-144=304$), ce qui entraîne de faibles frais supplémentaires à la fin de l'heure pour 304 crédits.

P6 – Pendant les 13 heures suivantes, l'utilisation de l'UC est à 5 % (niveau de référence). L'instance gagne autant de crédits qu'elle en dépense, sans excès pour rembourser progressivement le solde `CPUSurplusCreditBalance`. La valeur de `CPUSurplusCreditBalance` reste à 144 crédits.

P7 – Pendant les dernières 24 heures de cet exemple, l'instance est en veille et l'utilisation de l'UC est de 0 %. Pendant ce temps, l'instance gagne 144 crédits, qu'elle utilise pour rembourser progressivement le solde `CPUSurplusCreditBalance`.



Exemple 2 : Expliquer l'utilisation des crédits avec T2 illimité

Cet exemple montre l'utilisation de l'UC d'une instance `t2.nano` lancée en mode `unlimited` et comment l'instance dépense les crédits gagnés et excédentaires pour maintenir l'utilisation de l'UC.

Une instance `t2.nano` gagne 72 crédits UC sur une période glissante de 24 heures, qu'elle peut rembourser pour 72 minutes d'utilisation de processeur vCPU. Lorsqu'il épuise le solde créditeur de son processeur (représenté par la CloudWatch métrique `CPUCreditBalance`), il peut dépenser les crédits CPU excédentaires, qu'il n'a pas encore gagnés, pour augmenter aussi longtemps qu'il en a besoin. Comme une instance `t2.nano` gagne un maximum de 72 crédits sur une période de 24 heures, elle peut dépenser des crédits excédentaires jusqu'à ce maximum sans être facturée immédiatement. Si elle dépense plus de 72 crédits UC, la différence fait l'objet d'une facturation à la fin de l'heure.

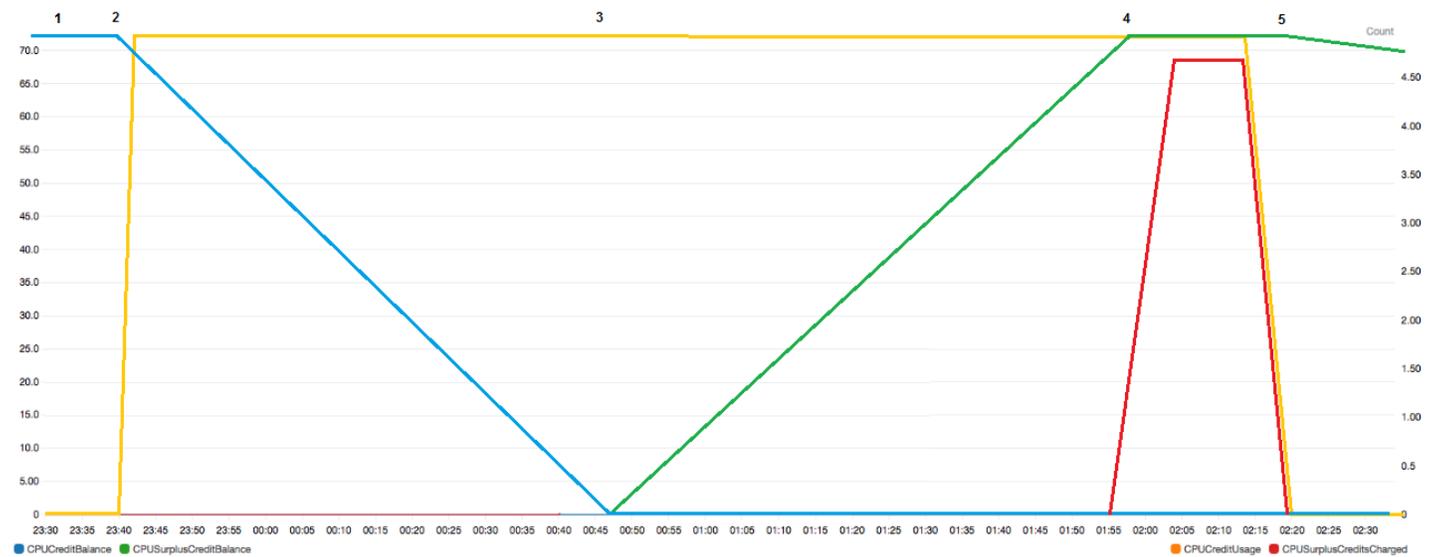
L'exemple illustré par le graphique suivant a pour but de montrer comment une instance peut passer en mode rafale à l'aide des crédits excédentaires, même après avoir épuisé son `CPUCreditBalance`. Vous pouvez supposer qu'au début de la ligne de temps du graphique, l'instance dispose d'un solde de crédits accumulés égal au nombre maximum de crédits qu'elle peut gagner en 24 heures. Le flux de travail suivant référence les points numérotés sur le graphique :

- 1 – Dans les 10 premières minutes, `CPUCreditUsage` est à 0, et la valeur de `CPUCreditBalance` reste à son maximum de 72.
- 2 – À 23h40, lorsque l'utilisation de l'UC augmente, l'instance dépense les crédits UC, et la valeur de `CPUCreditBalance` diminue.

3 – À 00 h 47, l'instance a épuisé l'intégralité de son `CPUCreditBalance` et commence à dépenser des crédits excédentaires pour maintenir l'utilisation élevée de l'UC.

4 – Les crédits excédentaires sont dépensés jusqu'à 01h55, lorsque la valeur de `CPU surplusCreditBalance` atteint 72 crédits UC. Cela équivaut au nombre maximum de crédits qu'une instance `t2.nano` peut gagner sur une période de 24 heures. Les crédits excédentaires dépensés par la suite ne peuvent pas être compensés par les crédits gagnés au cours de la période de 24 heures, ce qui entraîne de faibles frais supplémentaires à la fin de l'heure.

5 – L'instance continue de dépenser les crédits excédentaires jusqu'à 02h20 environ. À ce moment-là, l'utilisation de l'UC chute au-dessous du niveau de base, et l'instance commence à gagner des crédits à raison de 3 crédits par heure (soit 0,25 crédit toutes les 5 minutes), qu'elle utilise pour rembourser progressivement le `CPU surplusCreditBalance`. Une fois que la valeur de `CPU surplusCreditBalance` est nulle, l'instance commence à accumuler les crédits gagnés dans son `CPU creditBalance` à raison de 0,25 crédit toutes les 5 minutes.



Label	Details	Statistic	Period	Y Axis	Actions
CPUCreditBalance	EC2 • InstanceId:i-0aa4b948d7eb37d6b • CPUCreditBalance	Maximum	5 Minutes	< >	🔔 🔄 ⚙️
CPUCreditUsage	EC2 • InstanceId:i-0aa4b948d7eb37d6b • CPUCreditUsage	Maximum	5 Minutes	< >	🔔 🔄 ⚙️
CPUSurplusCreditBalance	EC2 • InstanceId:i-0aa4b948d7eb37d6b • CPUSurplusCreditBalance	Maximum	5 Minutes	< >	🔔 🔄 ⚙️
CPUSurplusCreditsCharged	EC2 • InstanceId:i-0aa4b948d7eb37d6b • CPUSurplusCreditsCharged	Maximum	5 Minutes	< >	🔔 🔄 ⚙️

Calcul de la facture (instance Linux)

Les crédits excédentaires coûtent 0,05\$ par heure de vCPU. L'instance a dépensé environ 25 crédits excédentaires entre 01h55 et 02h20, ce qui équivaut à 0,42 heure vCPU. Les frais supplémentaires pour cette instance sont de 0,42 heure de processeur virtuel x 0,05 \$/heure de processeur virtuel = 0,021 USD, arrondis à 0,02 USD. Facture de fin de mois correspondant à cette instance T2 illimité :

Amazon Elastic Compute Cloud running Linux/UNIX		
\$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	\$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
\$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	\$0.02

Calcul de la facture (instance Windows)

Les crédits excédentaires coûtent 0,096\$ par heure de processeur virtuel. L'instance a dépensé environ 25 crédits excédentaires entre 01h55 et 02h20, ce qui équivaut à 0,42 heure vCPU. Les frais supplémentaires pour cette instance sont de 0,42 heure de processeur virtuel x 0,096 \$/heure de processeur virtuel = 0,04032 USD, arrondis à 0,04 USD. Facture de fin de mois correspondant à cette instance T2 illimité :

Amazon Elastic Compute Cloud running Windows		
\$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	\$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
\$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	\$0.04

Vous pouvez définir des alertes de facturation pour être notifié toutes les heures des frais accumulés, puis prendre des mesures au besoin.

Mode standard pour les instances de performance à capacité extensible

Une instance de performance à capacité extensible configurée en mode standard est adaptée aux charges de travail avec une utilisation d'UC moyenne constamment inférieure à l'utilisation d'UC de référence de l'instance. Pour émettre en rafales au-dessus du niveau de base, l'instance dépense les crédits cumulés dans son solde de crédits UC. Si l'instance commence à manquer de crédits cumulés, son utilisation d'UC diminue progressivement pour atteindre le niveau d'utilisation de référence. Ainsi, l'instance ne subit pas une forte baisse des performances lorsque son solde de crédits UC est épuisé. Pour plus d'informations, consultez [Concepts et définitions clés pour les instances de performance à capacité extensible](#).

Sommaire

- [Concepts du mode standard](#)
- [Fonctionnement des instance de performance à capacité extensible standards](#)

- [Crédits de lancement](#)
- [Limites de crédits de lancement](#)
- [Différences entre crédits de lancement et crédits gagnés](#)
- [Exemples de mode standard](#)
 - [Exemple 1 : Expliquer l'utilisation des crédits avec T3 standard](#)
 - [Exemple 2 : Expliquer l'utilisation des crédits avec T2 standard](#)
 - [Période 1 : 1 – 24 heures](#)
 - [Période 2 : 25 – 36 heures](#)
 - [Période 3 : 37 – 61 heures](#)
 - [Période 4 : 62 – 72 heures](#)
 - [Période 5 : 73 – 75 heures](#)
 - [Période 6 : 76 – 90 heures](#)
 - [Période 7 : 91 – 96 heures](#)

Concepts du mode standard

Le mode standard est une option de configuration pour les instances de performance à capacité extensible. Il peut être activé ou désactivé à tout moment pour une instance en cours d'exécution ou arrêtée. Vous pouvez [la définir standard comme option de crédit par défaut](#) au niveau du compte, par AWS région, par famille d'instances de performance éclatante, afin que toutes les nouvelles instances de performance actualisées du compte soient lancées à l'aide de l'option de crédit par défaut.

Fonctionnement des instance de performance à capacité extensible standards

Lorsqu'une instance de performance à capacité extensible configurée en mode standard est en cours d'exécution, elle gagne continuellement (à une résolution de l'ordre de la milliseconde) un taux déterminé de crédits gagnés par heure. Lorsqu'une instance T2 Standard est arrêtée, elle perd tous ses crédits accumulés et le solde de crédits est remis à zéro. Lorsqu'elle est redémarrée, elle reçoit un nouveau jeu de crédits de lancement, et commence à accumuler des crédits gagnés. Pour les instances Standard T4g, T3a et T3, le solde de crédits d'UC est conservé pendant sept jours après l'arrêt de l'instance. Ensuite, les crédits sont perdus. Si vous démarrez l'instance dans les sept jours, aucun crédit n'est perdu.

Les instances T2 standard reçoivent deux types de [crédits UC](#) : les crédits gagnés et les crédits de lancement. Lorsqu'une instance T2 Standard est en cours d'exécution, elle gagne continuellement (à une résolution de l'ordre de la milliseconde) un taux déterminé de crédits gagnés par heure. Au début, elle n'a pas de crédits gagnés pour une bonne expérience de démarrage ; elle reçoit donc, à cet effet, des crédits de lancement, qui sont dépensés pendant qu'elle accumule des crédits gagnés.

Les instances T4g, T3a et T3 ne reçoivent pas de crédits de lancement parce qu'elles prennent en charge le mode Illimité. La configuration du crédit en mode illimité permet aux instances T4g, T3a et T3 d'utiliser autant d'UC que nécessaire pour dépasser la ligne de référence aussi longtemps que nécessaire.

Crédits de lancement

Les instances T2 Standard reçoivent 30 crédits de lancement par vCPU au lancement ou au démarrage, et les instances T1 Standard reçoivent 15 crédits de lancement. Par exemple, une instance `t2.micro` compte un processeur vCPU et obtient 30 crédits de lancement tandis qu'une instance `t2.xlarge` possède quatre processeurs vCPU et obtient 120 crédits de lancement. Les crédits de lancement sont conçus pour fournir une bonne expérience de démarrage et permettre aux instances de s'exécuter en mode rafale dès le lancement, avant qu'elles aient accumulé des crédits gagnés.

Les crédits de lancement sont dépensés en premier, avant les crédits gagnés. Les crédits de lancement non dépensés sont accumulés dans le solde de crédits UC, mais ne sont pas comptés dans la limite du solde de crédits UC. Par exemple, une instance `t2.micro` comporte une limite de solde de crédits UC de 144 crédits gagnés. Si elle est lancée et reste inactive pendant 24 heures, son solde de crédits UC atteint 174 (30 crédits de lancement + 144 crédits gagnés), ce qui se situe au-delà de la limite. Toutefois, une fois que l'instance a dépensé les 30 crédits de lancement, le solde de crédits ne peut pas excéder 144. Pour en savoir plus sur la limite du solde de crédits pour l'UC par rapport à chaque taille d'instance, consultez le [tableau des crédits](#).

Le tableau suivant répertorie l'allocation de crédits UC initiale reçus au lancement ou au démarrage, ainsi que le nombre de processeurs vCPU.

Type d'instance	Crédits de lancement	vCPU
<code>t1.micro</code>	15	1
<code>t2.nano</code>	30	1

Type d'instance	Crédits de lancement	vCPU
t2.micro	30	1
t2.small	30	1
t2.medium	60	2
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

Limites de crédits de lancement

Le nombre de fois où les instances T2 Standard peuvent recevoir des crédits de lancement est limité. La limite par défaut est définie sur 100 lancements ou démarrages de toutes les instances T2 Standard combinées par compte, par région et par déploiement de 24 heures. Par exemple, la limite est atteinte lorsqu'une instance est arrêtée et démarrée 100 fois sur une période de 24 heures, ou lorsque 100 instances sont lancées sur une période de 24 heures, ou toute autre combinaison équivalente à 100 démarrages. Les nouveaux comptes peuvent présenter une limite inférieure qui augmentera au fil du temps en fonction de votre utilisation.

Tip

Pour vous assurer que vos charges de travail obtiennent toujours les performances nécessaires, passez à une instance [Mode illimité pour les instances de performance à capacité extensible](#) ou utilisez une taille d'instance supérieure.

Différences entre crédits de lancement et crédits gagnés

Le tableau suivant répertorie les différences entre les crédits de lancement et les crédits gagnés.

	Crédits de lancement	Crédits gagnés
Taux d'obtention de crédits	<p>Les instances T2 Standard obtiennent 30 crédits de lancement par processeur vCPU au lancement ou au démarrage.</p> <p>Si une instance T2 bascule du mode <code>unlimited</code> au mode <code>standard</code>, elle n'obtient pas de crédits de lancement au moment du basculement.</p>	<p>Chaque instance T2 gagne continuellement (à une résolution de l'ordre de la milliseconde) un taux déterminé de crédits UC par heure, en fonction de sa taille. Pour plus d'informations sur le nombre de crédits pour l'UC gagnés par taille d'instance, consultez le tableau des crédits.</p>
Limite d'obtention de crédits	<p>La limite pour la réception de crédits de lancement est définie sur 100 lancements ou démarrages de toutes les instances T2 Standard combinées par compte, par région et par déploiement de 24 heures. Les nouveaux comptes peuvent présenter une limite inférieure qui augmentera au fil du temps en fonction de votre utilisation.</p>	<p>Une instance T2 ne peut pas accumuler davantage de crédits que la limite du solde de crédits UC. Si le solde de crédits UC a atteint sa limite, les crédits gagnés une fois que la limite a été atteinte sont détruits. Les crédits de lancement ne sont pas comptés dans la limite. Pour en savoir plus sur la limite du solde de crédits pour l'UC pour chaque taille d'instance T2, consultez le tableau des crédits.</p>
Utilisation des crédits	<p>Les crédits de lancement sont dépensés en premier, avant les crédits gagnés.</p>	<p>Les crédits gagnés sont dépensés uniquement lorsque tous les crédits de lancement ont été dépensés.</p>
Expiration des crédits	<p>Les crédits de lancement d'une instance T2 Standard en cours d'exécution n'expirent pas. Lorsqu'une instance T2 Standard s'arrête ou passe à T2 illimité, tous les crédits de lancement sont perdus.</p>	<p>Lorsqu'une instance T2 est en cours d'exécution, les crédits gagnés qui ont été accumulés n'expirent pas. Lorsque l'instance T2 s'arrête, tous les crédits gagnés accumulés sont perdus.</p>

Le nombre de crédits de lancement accumulés et de crédits accumulés est suivi par la métrique `CloudWatch CPUcreditBalance`. Pour plus d'informations, consultez [CPUcreditBalance](#) le [tableau CloudWatch des mesures](#).

Exemples de mode standard

Les exemples suivants expliquent l'utilisation des crédits lorsque des instances sont configurées en mode standard.

Exemples

- [Exemple 1 : Expliquer l'utilisation des crédits avec T3 standard](#)
- [Exemple 2 : Expliquer l'utilisation des crédits avec T2 standard](#)

Exemple 1 : Expliquer l'utilisation des crédits avec T3 standard

Cet exemple vous montre comment une instance `t3.nano` lancée en mode standard gagne, accumule et dépense des crédits gagnés. Vous pouvez voir que le solde de crédits reflète les crédits gagnés accumulés.

Une instance `t3.nano` en cours d'exécution gagne 144 crédits toutes les 24 heures. Sa limite de solde de crédits est de 144 crédits gagnés. Une fois que la limite est atteinte, les nouveaux crédits gagnés sont rejetés. Pour plus d'informations sur le nombre de crédits pour l'UC pouvant être gagnés et accumulés, consultez le [tableau des crédits](#).

Vous pouvez lancer une instance T3 Standard et l'utiliser immédiatement. Ou vous pouvez lancer une instance T3 Standard et la laisser inactive pendant quelques jours avant d'y exécuter des applications. L'utilisation ou l'inactivité d'une instance détermine si les crédits sont accumulés ou dépensés. Si une instance reste inactive pendant 24 heures après son lancement, le solde de crédits atteint sa limite, qui correspond au nombre maximal de crédits gagnés qui peuvent être accumulés.

Cet exemple décrit une instance qui reste inactive pendant 24 heures après son lancement, et explique sept périodes sur une plage de 96 heures. L'exemple illustre les taux d'obtention, d'accumulation, de dépense et de rejet de crédits, ainsi que la valeur du solde de crédits à la fin de chaque période.

Le flux de travail suivant référence les points numérotés sur le graphique :

P1 – À 0 heure sur le graphe, l'instance est lancée en mode standard et commence immédiatement à gagner des crédits. L'instance reste inactive après son lancement (l'utilisation de l'UC est de

0 %) et aucun crédit n'est dépensé. Tous les crédits non dépensés sont accumulés dans le solde de crédits. Pendant les premières 24 heures, `CPUCreditUsage` est à 0 et la valeur de `CPUCreditBalance` atteint son maximum de 144.

P2 – Pendant les 12 heures suivantes, l'utilisation de l'UC est à 2,5 %, ce qui est inférieur au niveau de référence de 5 %. L'instance gagne plus de crédits qu'elle n'en dépense, mais la valeur de `CPUCreditBalance` ne peut pas dépasser son maximum de 144 crédits. Tous les crédits gagnés au-delà de cette limite sont rejetés.

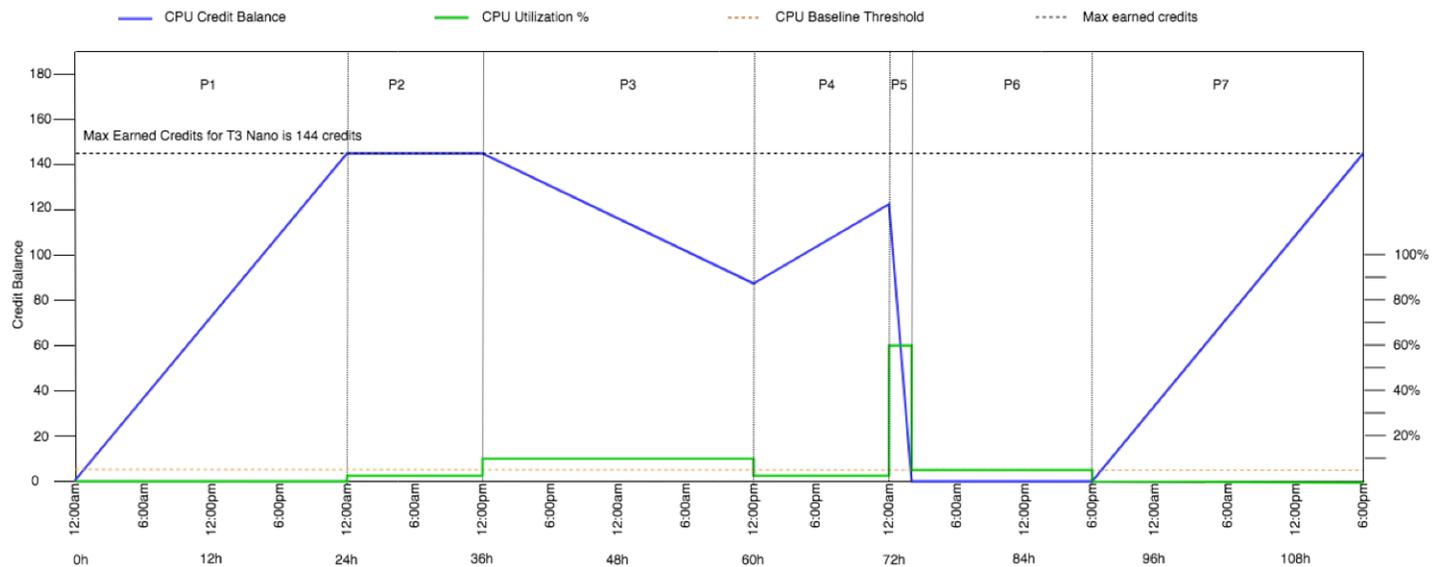
P3 – Pendant les 24 heures suivantes, l'utilisation de l'UC est de 7 % (au-dessus du niveau de référence), ce qui nécessite la dépense de 57,6 crédits. L'instance dépense plus de crédits qu'elle n'en gagne et la valeur de `CPUCreditBalance` baisse jusqu'à 86,4 crédits.

P4 – Pendant les 12 heures suivantes, l'utilisation de l'UC baisse jusqu'à 2,5 % (sous le niveau de référence), ce qui nécessite la dépense de 36 crédits. Au même moment, l'instance gagne 72 crédits. L'instance gagne plus de crédits qu'elle n'en dépense et la valeur `CPUCreditBalance` augmente jusqu'à 122 crédits.

P5 – Pendant les deux heures suivantes, l'instance est à un pic de 60 % d'utilisation de l'UC et épuise sa valeur de `CPUCreditBalance` complète de 122 crédits. À la fin de cette période, la valeur de `CPUCreditBalance` est nulle et l'utilisation de l'UC est obligée de baisser jusqu'au niveau d'utilisation de référence de 5 %. Au niveau de base, l'instance gagne autant de crédits qu'elle en dépense.

P6 – Pendant les 14 heures suivantes, l'utilisation de l'UC est à 5 % (niveau de référence). L'instance gagne autant de crédits qu'elle en dépense. La valeur de `CPUCreditBalance` reste à 0.

P7 – Pendant les dernières 24 heures de cet exemple, l'instance est en veille et l'utilisation de l'UC est de 0 %. Pendant ce temps, l'instance gagne 144 crédits, qu'elle accumule dans son solde `CPUCreditBalance`.



Exemple 2 : Expliquer l'utilisation des crédits avec T2 standard

Cet exemple vous montre comment une instance t2.nano lancée en tant que standard gagne, accumule et dépense des crédits de lancement et des crédits gagnés. Vous pouvez voir que le solde de crédits reflète non seulement les crédits gagnés accumulés, mais également les crédits de lancement accumulés.

Une instance t2.nano obtient 30 crédits de lancement lorsqu'elle est lancée, et gagne 72 crédits par 24 heures. Sa limite du solde de crédits est de 72 crédits gagnés ; les crédits de lancement ne sont pas comptés dans la limite. Une fois que la limite est atteinte, les nouveaux crédits gagnés sont rejetés. Pour plus d'informations sur le nombre de crédits pour l'UC pouvant être gagnés et accumulés, consultez le [tableau des crédits](#). Pour en savoir plus sur les limites, consultez [Limites de crédits de lancement](#).

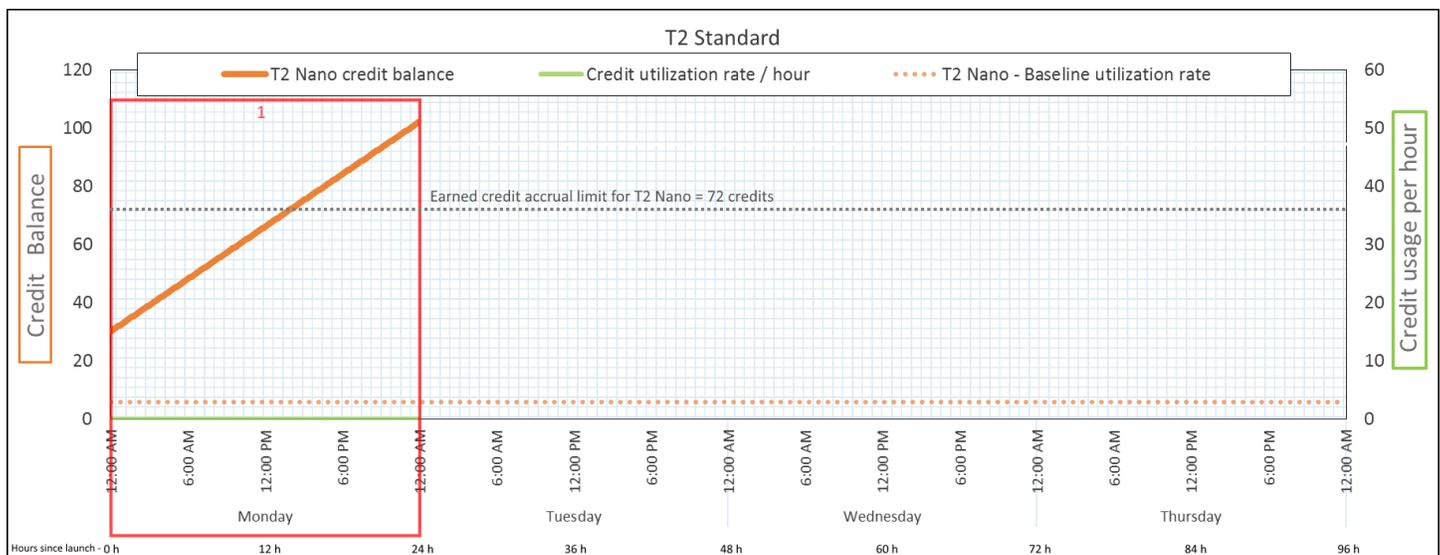
Vous pouvez lancer une instance T2 Standard et l'utiliser immédiatement. Ou vous pouvez lancer une instance T2 Standard et la laisser inactive pendant quelques jours avant d'y exécuter des applications. L'utilisation ou l'inactivité d'une instance détermine si les crédits sont accumulés ou dépensés. Si une instance reste inactive pendant 24 heures après son lancement, le solde de crédits est affiché comme dépassant sa limite, car le solde reflète à la fois les crédits gagnés accumulés et les crédits de lancement accumulés. Cependant, après l'utilisation de l'UC, les crédits de lancement sont dépensés en premier. Par la suite, la limite reflète toujours le nombre maximum de crédits gagnés pouvant être accumulés.

Cet exemple décrit une instance qui reste inactive pendant 24 heures après son lancement, et explique sept périodes sur une plage de 96 heures. L'exemple illustre les taux d'obtention,

d'accumulation, de dépense et de rejet de crédits, ainsi que la valeur du solde de crédits à la fin de chaque période.

Période 1 : 1 – 24 heures

À 0 heure sur le graphe, l'instance T2 est lancée en tant que `standard` et obtient immédiatement 30 crédits de lancement. Elle gagne des crédits lorsqu'elle s'exécute. L'instance reste inactive après son lancement (l'utilisation de l'UC est de 0 %) et aucun crédit n'est dépensé. Tous les crédits non dépensés sont accumulés dans le solde de crédits. Environ 14 heures après le lancement, le solde de crédits est de 72 (30 crédits de lancement + 42 crédits gagnés), ce qui équivaut à ce que l'instance peut gagner en 24 heures. 24 heures après le lancement, le solde de crédits dépasse 72 crédits, car les crédits de lancement non dépensés sont inclus dans le —solde de crédits. Le solde de crédits est de 102 crédits : 30 crédits de lancement + 72 crédits gagnés.



Taux de dépense de crédits

0 crédits par 24 heures (utilisation de l'UC 0 %)

Taux d'obtention de crédits

72 crédits par 24 heures

Taux de rejet de crédits

0 crédits par 24 heures

Solde de crédits

102 crédits (30 crédits de lancement + 72 crédits gagnés)

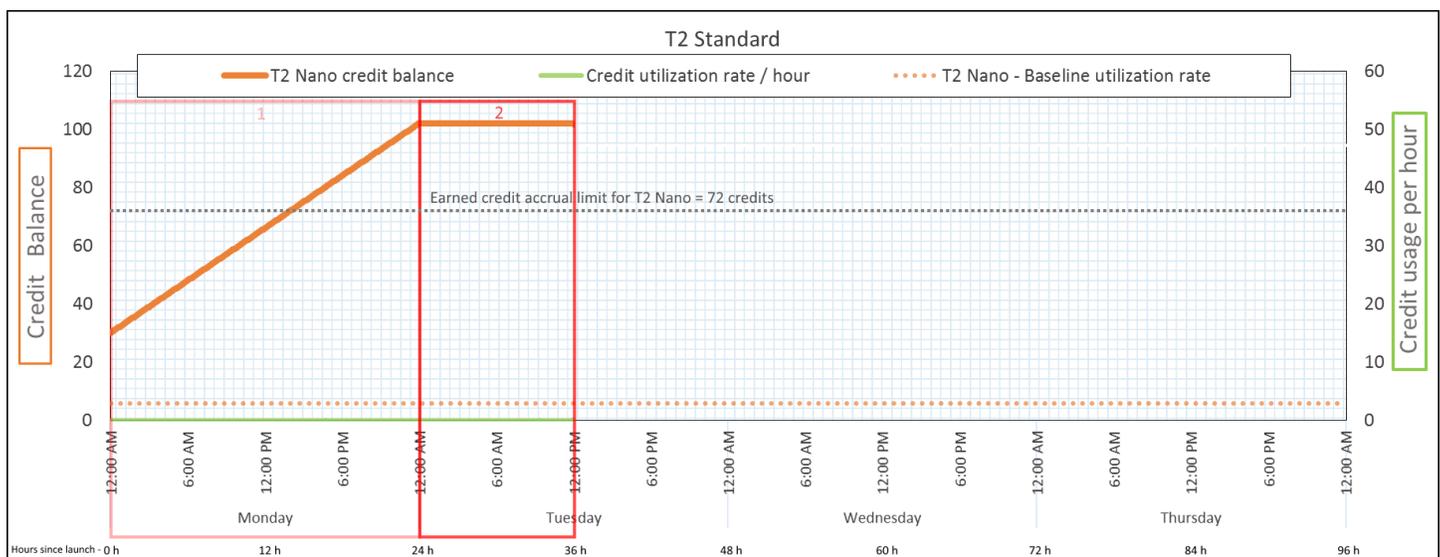
Conclusion

Si l'UC n'est pas utilisée après le lancement, l'instance accumule plus de crédits qu'elle ne peut en gagner en 24 heures (30 crédits de lancement + 72 crédits gagnés = 102 crédits).

Dans un scénario réel, une instance EC2 utilise quelques crédits pendant le lancement et l'exécution, ce qui évite que le solde atteigne la valeur théorique maximale dans cet exemple.

Période 2 : 25 – 36 heures

Pendant les 12 heures suivantes, l'instance reste encore inactive et gagne des crédits, mais le solde de crédits n'augmente pas. Il se stabilise à 102 crédits (30 crédits de lancement + 72 crédits gagnés). Le solde de crédits a atteint sa limite de 72 crédits gagnés accumulés. C'est pour cette raison que les nouveaux crédits gagnés sont rejetés.



Taux de dépense de crédits

0 crédits par 24 heures (utilisation de l'UC 0 %)

Taux d'obtention de crédits

72 crédits par 24 heures (3 crédits par heure)

Taux de rejet de crédits

72 crédits par 24 heures (100 % du taux d'obtention de crédits)

Solde de crédits

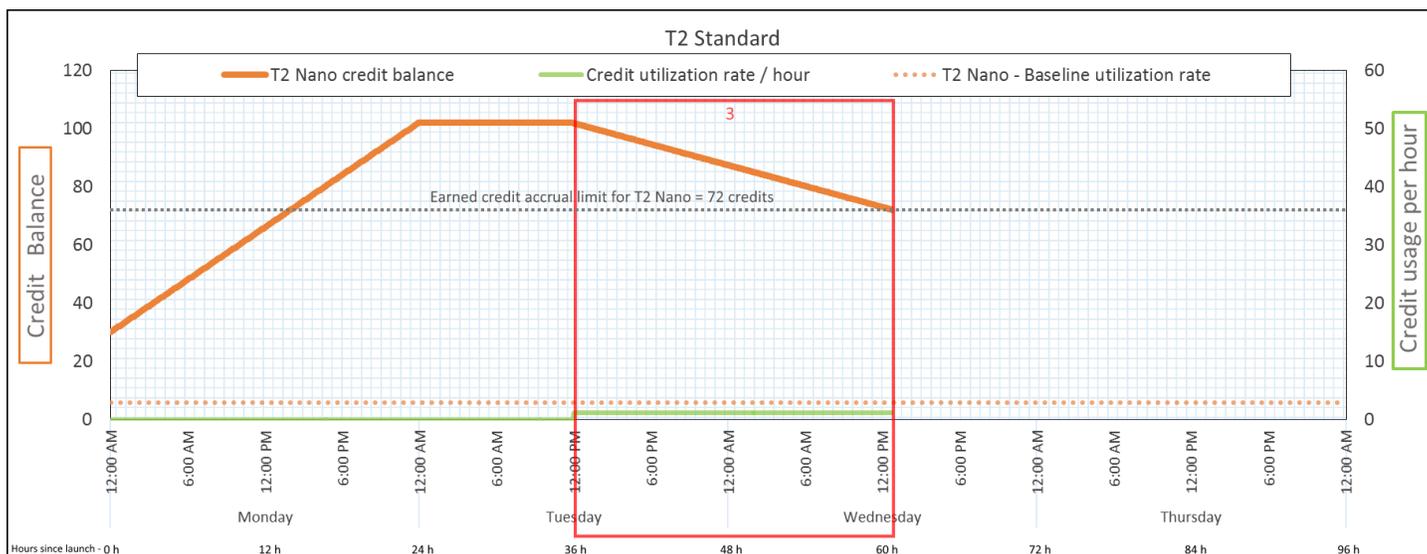
102 crédits (30 crédits de lancement + 72 crédits gagnés) — le solde est inchangé

Conclusion

Une instance gagne des crédits en permanence, mais elle ne peut pas accumuler des crédits gagnés au-delà de la limite du solde de crédits. Une fois que la limite est atteinte, les nouveaux crédits gagnés sont rejetés. Les crédits de lancement ne sont pas comptés dans la limite du solde de crédits. Si le solde comprend les crédits de lancement accumulés, il est affiché comme dépassant la limite.

Période 3 : 37 – 61 heures

Pendant les 25 heures suivantes, l'instance utilise 2 % d'UC, ce qui équivaut à 30 crédits. Pendant ce même laps de temps, elle gagne 75 crédits, mais le solde de crédits diminue. Le solde diminue car les crédits de lancement accumulés sont dépensés en premier, et les nouveaux crédits gagnés sont rejetés, car le solde de crédits a déjà atteint sa limite de 72 crédits gagnés.



Taux de dépense de crédits

28,8 crédits par 24 heures (1,2 crédits par heure, utilisation de l'UC de 2 %, 40 % du taux d'obtention de crédits) : 30 crédits sur 25 heures

Taux d'obtention de crédits

72 crédits par 24 heures

Taux de rejet de crédits

72 crédits par 24 heures (100 % du taux d'obtention de crédits)

Solde de crédits

72 crédits (30 crédits de lancement ont été dépensés ; 72 crédits gagnés n'ont pas été dépensé)

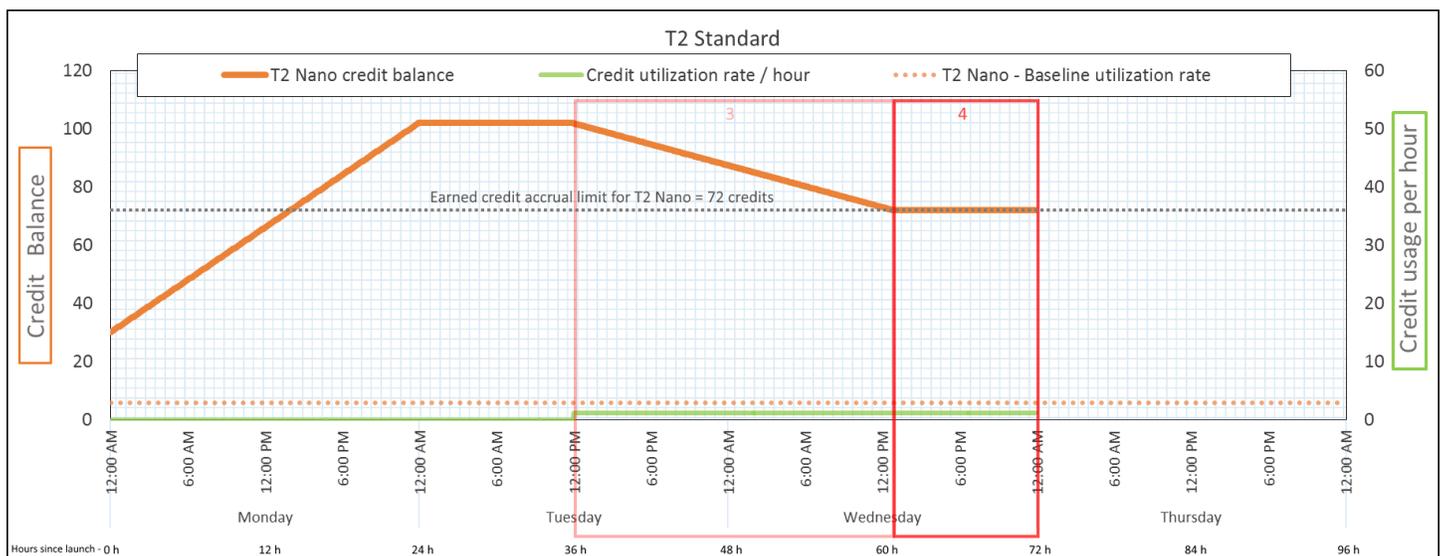
Conclusion

Une instance dépense les crédits de lancement en premier, avant les crédits gagnés. Les crédits de lancement ne sont pas comptés dans la limite de crédits. Lorsque les crédits de lancement sont dépensés, le solde ne peut pas être plus élevé que ce qui peut être gagné en l'espace de 24 heures. De plus, lorsqu'une instance s'exécute, elle ne peut pas obtenir de nouveaux crédits de lancement.

Période 4 : 62 – 72 heures

Pendant les 11 heures suivantes, l'instance utilise 2 % d'UC, ce qui équivaut à 13.2 crédits. Cette utilisation de l'UC est identique à celle de la période précédente, mais le solde ne diminue pas. Il reste à 72 crédits.

Le solde ne diminue pas, car le taux d'obtention de crédits est supérieur à celui de dépense de crédits. Pendant que l'instance dépense 13.2 crédits, elle en gagne également 33. Cependant, la limite du solde étant de 72 crédits, les éventuels crédits gagnés au-delà de la limite sont rejetés. Le solde se stabilise à 72 crédits, et non à 102 crédits comme lors de la deuxième période, car il n'y a aucun crédit de lancement accumulé.



Taux de dépense de crédits

28,8 crédits par 24 heures (1,2 crédits par heure, utilisation de l'UC de 2 %, 40 % du taux d'obtention de crédits) : 13,2 crédits sur 11 heures

Taux d'obtention de crédits

72 crédits par 24 heures

Taux de rejet de crédits

43.2 crédits par 24 heures (60 % du taux d'obtention de crédits)

Solde de crédits

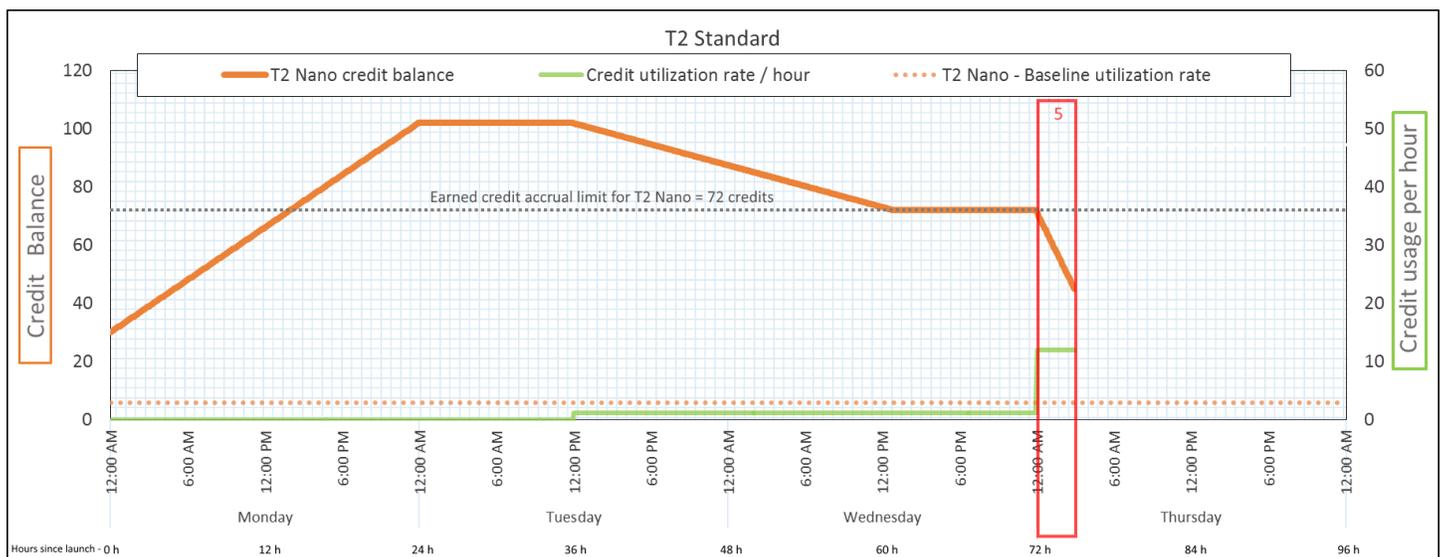
72 crédits (0 crédit de lancement, 72 crédits gagnés) — le solde atteint sa limite

Conclusion

Une fois que les crédits de lancement sont dépensés, la limite du solde de crédits est déterminée par le nombre de crédits qu'une instance peut gagner en l'espace de 24 heures. Si l'instance gagne plus de crédits qu'elle n'en dépense, les nouveaux crédits gagnés au-delà de la limite sont rejetés.

Période 5 : 73 – 75 heures

Pendant les trois heures suivantes, l'utilisation de l'UC de l'instance passe à 20 %, ce qui équivaut à 36 crédits. L'instance gagne neuf crédits au cours de ces trois heures, ce qui entraîne une diminution du solde de 27 crédits. Au terme des trois heures, le solde de crédits est de 45 crédits gagnés accumulés.



Taux de dépense de crédits

288 crédits par 24 heures (12 crédits par heure, utilisation de l'UC de 20 %, 400 % du taux d'obtention de crédits) — 36 crédits sur 3 heures)

Taux d'obtention de crédits

72 crédits par 24 heures (9 crédits en 3 heures)

Taux de rejet de crédits	0 crédits par 24 heures
Solde de crédits	45 crédits (solde précédent (72) - crédits dépensés (36) + crédits gagnés (9)) — le solde diminue à 216 crédits par 24 heures (taux de dépense 288/24 + taux d'obtention 72/24 = taux de diminution du solde 216/24)

Conclusion

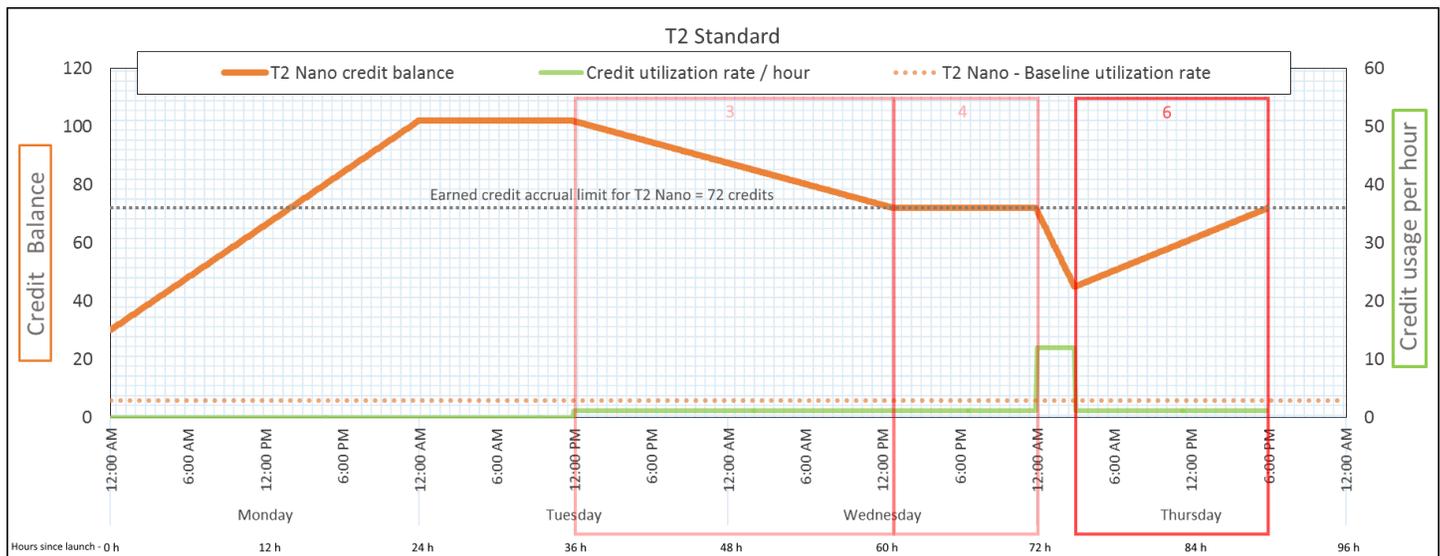
Si une instance dépense plus de crédits qu'elle n'en gagne, son solde de crédits diminue.

Période 6 : 76 – 90 heures

Pendant les 15 heures suivantes, l'instance utilise 2 % d'UC, ce qui équivaut à 18 crédits. L'utilisation est la même que celle des périodes 3 et 4. Cependant, le solde augmente au cours de cette période, alors qu'il avait diminué pendant la troisième période, et s'était stabilisé pendant la quatrième.

Pendant la troisième période, les crédits de lancement accumulés avaient été dépensés et les crédits gagnés au-delà de la limite de crédits avaient été rejetés, ce qui explique la diminution du solde de crédits. Pendant la quatrième période, l'instance avait dépensé moins de crédits qu'elle n'en avait gagné. Les crédits gagnés au-delà de la limite ont été rejetés, ce qui explique la stabilisation du solde à 72 crédits.

Au cours de cette nouvelle période, il n'y a aucun crédit de lancement accumulé, et le nombre de crédits gagnés accumulés du solde est inférieur à la limite. Aucun crédit gagné n'est rejeté. De plus, l'instance gagne plus de crédits qu'elle n'en dépense, ce qui entraîne une augmentation du solde de crédits.



Taux de dépense de crédits

28,8 crédits par 24 heures (1,2 crédits par heure, utilisation de l'UC de 2 %, 40 % du taux d'obtention de crédits) — 18 crédits sur 15 heures

Taux d'obtention de crédits

72 crédits par 24 heures (45 crédits en 15 heures)

Taux de rejet de crédits

0 crédits par 24 heures

Solde de crédits

72 crédits (le solde augmente à un taux de 43,2 crédits par 24 heures — taux de variation = taux de dépense 28,8/24 + taux d'obtention 72/24)

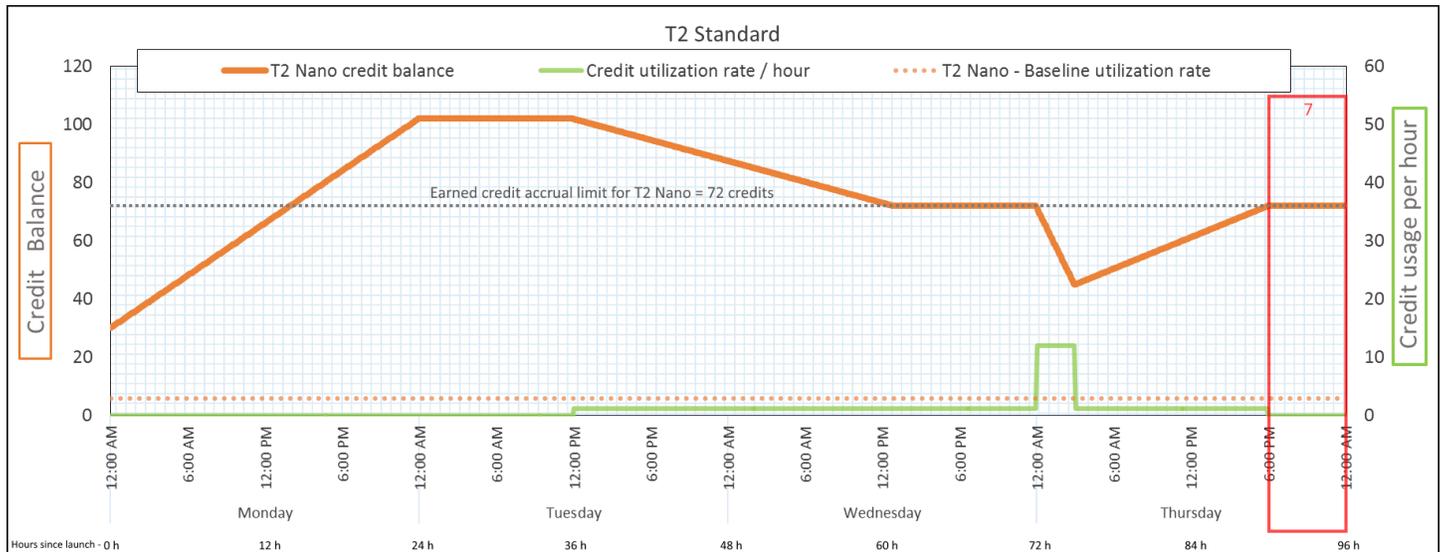
Conclusion

Si une instance dépense moins de crédits qu'elle n'en gagne, son solde de crédits augmente.

Période 7 : 91 – 96 heures

Pendant les six heures suivantes, l'instance— reste inactive – l'utilisation— de l'UC est 0 % – et aucun crédit n'est dépensé. L'utilisation de l'UC est identique à celle de la deuxième période, mais le solde ne se stabilise pas à 102 crédits. Il se stabilise— à 72 crédits, soit la limite du solde de crédits de l'instance.

Au cours de la deuxième période, le solde de crédits comprenait 30 crédits de lancement accumulés. Les crédits de lancement ont été dépensés au cours de la troisième période. Une instance en cours d'exécution ne peut pas obtenir d'autres crédits de lancement. Lorsque la limite du solde de crédits est atteinte, les éventuels crédits gagnés au-delà de la limite sont rejetés.



Taux de dépense de crédits	0 crédits par 24 heures (utilisation de l'UC 0 %)
Taux d'obtention de crédits	72 crédits par 24 heures
Taux de rejet de crédits	72 crédits par 24 heures (100 % du taux d'obtention de crédits)
Solde de crédits	72 crédits (0 crédit de lancement + 72 crédits gagnés)

Conclusion

Une instance gagne des crédits en permanence, mais ne peut pas accumuler des crédits gagnés si la limite du solde de crédits est atteinte. Une fois que la limite est atteinte, les nouveaux crédits gagnés sont rejetés. La limite du solde de crédits est déterminée par le nombre de crédits qu'une instance peut gagner en l'espace de 24 heures. Pour plus d'informations sur les limites du solde de crédits, consultez le [tableau des crédits](#).

Utiliser des instance de performance à capacité extensible

Les étapes de lancement, de surveillance et de modification des instances de performance en rafale (instances T) sont similaires. La différence clé est la spécification de crédits par défaut lors de leur lancement :

Chaque famille d'instances T est fournie avec la spécification de crédit par défaut suivante :

- Les instances T4g, T3a et T3 sont lancées en tant que `unlimited`
- Les instances T3 sur un hôte dédié ne peuvent être lancées qu'en tant que `standard`
- Instances T2 lancées en mode `standard`

Vous pouvez [modifier la spécification de crédit par défaut](#) pour le compte.

Table des matières

- [Lancer une instance de performance à capacité extensible en mode Illimité ou Standard](#)
- [Utiliser un groupe Auto Scaling pour lancer une instance de performance à capacité extensible en mode Illimité](#)
- [Afficher la spécification de crédits d'une instance de performance à capacité extensible](#)
- [Modifier la spécification de crédits d'une instance de performance à capacité extensible](#)
- [Définir la spécification de crédits par défaut pour le compte](#)
- [Afficher la spécification de crédits par défaut](#)

Lancer une instance de performance à capacité extensible en mode Illimité ou Standard

Vous pouvez lancer vos instances T en tant que `unlimited` ou `standard` en utilisant la console Amazon EC2, un AWS SDK, un outil de ligne de commande ou avec un groupe Auto Scaling.

Les procédures suivantes décrivent comment utiliser la console EC2 ou le AWS CLI. Pour plus d'informations sur l'utilisation d'un groupe Auto Scaling, consultez [Utiliser un groupe Auto Scaling pour lancer une instance de performance à capacité extensible en mode Illimité](#).

Console

Pour lancer une instance T en tant que version illimitée ou standard

1. Suivez la procédure pour [lancer une instance](#).

2. Pour Instance type (Type d'Instance), sélectionnez un type d'instance T.
3. Développez Advanced details (Détails avancés), et pour Credit specification (Spécification de crédit), sélectionnez une spécification de crédit. Si vous n'effectuez aucune sélection, la valeur par défaut est utilisée, c'est-à-dire standard pour T2, T4g, T3a et T3. unlimited
4. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

AWS CLI

Pour lancer une instance T en tant que version illimitée ou standard

Utilisez la commande [run-instances](#) pour lancer vos instances. Spécifiez la spécification de crédits à l'aide du paramètre `--credit-specification CpuCredits=`. Les spécifications de crédits valides sont `unlimited` et `standard`.

- Pour T4g, T3a et T3, si vous n'incluez pas le `--credit-specification` paramètre, l'instance se lance comme `unlimited` par défaut.
- Pour T2, si vous n'incluez pas le paramètre `--credit-specification`, l'instance est lancée en mode `standard` par défaut.

```
aws ec2 run-instances \  
  --image-id ami-abc12345 \  
  --count 1 \  
  --instance-type t3.micro \  
  --key-name MyKeyPair \  
  --credit-specification "CpuCredits=unlimited"
```

Utiliser un groupe Auto Scaling pour lancer une instance de performance à capacité extensible en mode Illimité

Lorsque les instances T sont lancées ou démarrées, elles ont besoin de crédits CPU pour une bonne expérience d'amorçage. Si vous utilisez un groupe Auto Scaling pour lancer vos instances, nous vous conseillons de configurer vos instances en mode `unlimited`. Dans ce cas, elles utilisent les crédits excédentaires en cas de lancement ou de redémarrage automatique par le groupe Auto Scaling. L'utilisation des crédits excédentaires empêche les restrictions de performances.

Créer un modèle de lancement

Vous devez utiliser un modèle de lancement pour lancer les instances en mode `unlimited` dans un groupe Auto Scaling. Une configuration de lancement ne prend pas en charge le lancement des instances en mode `unlimited`.

Note

Le mode `unlimited` n'est pas pris en charge pour les instances T3 lancées sur un hôte dédié.

Console

Pour créer un modèle de lancement des instances en mode Illimité

1. Suivez la procédure de [création d'un modèle de lancement à l'aide des paramètres avancés](#) du guide de l'utilisateur Amazon EC2 Auto Scaling.
2. Dans Launch template contents (Contenu du modèle de lancement), pour Instance type (Type d'instance), choisissez une taille d'instance.
3. Pour lancer des instances en mode `unlimited` dans un groupe Auto Scaling, sous Advanced details (Détails avancés), pour la Credit specification (Spécification de crédits), choisissez Unlimited (Illimité).
4. Lorsque vous avez fini de définir les paramètres de modèle de lancement, choisissez Créer un modèle de lancement.

AWS CLI

Pour créer un modèle de lancement des instances en mode Illimité

Utilisez la commande [create-launch-template](#) et spécifiez `unlimited` comme spécification de crédits.

- Pour T4g, T3a et T3, si vous n'incluez pas la `CreditSpecification={CpuCredits=unlimited}` valeur, l'instance est lancée par défaut. `unlimited`

- Pour T2, si vous n'incluez pas la valeur `CreditSpecification={CpuCredits=unlimited}`, l'instance est lancée en mode standard par défaut.

```
aws ec2 create-launch-template \  
  --launch-template-name MyLaunchTemplate \  
  --version-description FirstVersion \  
  --launch-template-data  
ImageId=ami-8c1be5f6,InstanceType=t3.medium,CreditSpecification={CpuCredits=unlimited}
```

Associer un groupe Auto Scaling avec un modèle de lancement

Pour associer le modèle de lancement à un groupe Auto Scaling, créez le groupe Auto Scaling à l'aide du modèle de lancement ou ajoutez le modèle de lancement à un groupe Auto Scaling existant.

Console

Pour créer un groupe Auto Scaling à l'aide d'un modèle de lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation située en haut de l'écran, sélectionnez la même région que celle utilisée lorsque vous avez créé le modèle de lancement.
3. Dans le panneau de navigation, choisissez Groupes Auto Scaling, puis Créer le groupe Auto Scaling.
4. Choisissez Modèle de lancement, sélectionnez votre modèle de lancement, puis choisissez Étape suivante.
5. Complétez les champs pour le groupe Auto Scaling. Lorsque vous avez fini de passer en revue vos paramètres de configuration sur la page Vérification, choisissez Créer le groupe Auto Scaling. Pour plus d'informations, consultez [Création d'un groupe Auto Scaling à l'aide d'un modèle de lancement](#) dans le Amazon EC2 Auto Scaling Guide de l'utilisateur.

AWS CLI

Pour créer un groupe Auto Scaling à l'aide d'un modèle de lancement

Utilisez la AWS CLI commande [create-auto-scaling-group](#) et spécifiez le paramètre. `--launch-template`

Console

Pour ajouter un modèle de lancement à un groupe Auto Scaling existant

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation située en haut de l'écran, sélectionnez la même région que celle utilisée lorsque vous avez créé le modèle de lancement.
3. Dans le panneau de navigation, choisissez Groupes Auto Scaling.
4. Dans la liste des groupes Auto Scaling, sélectionnez un groupe Auto Scaling et choisissez Actions, Modifier.
5. Sous l'onglet Détails, pour Modèle de lancement, choisissez un modèle de lancement, puis choisissez Enregistrer.

AWS CLI

Pour ajouter un modèle de lancement à un groupe Auto Scaling existant

Utilisez la AWS CLI commande [update-auto-scaling-group](#) et spécifiez le paramètre. `--launch-template`

Afficher la spécification de crédits d'une instance de performance à capacité extensible

Vous pouvez consulter la spécification de crédit (`unlimited` ou `standard`) d'une instance T en cours d'exécution ou arrêtée.

Console

Pour consulter la spécification de crédit d'une instance T

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, choisissez Instances.
3. Sélectionnez l'instance.
4. Choisissez Détails (Détails) et affichez le champ Credit specification (Spécification de crédits). La valeur est `unlimited` ou `standard`.

AWS CLI

Pour décrire la spécification de crédit d'une instance T

Utilisez la commande [describe-instance-credit-specifications](#). Si vous ne spécifiez aucun ID d'instance, toutes les instances avec la spécification de crédits `unlimited` sont retournées, ainsi que les instances qui ont été précédemment configurées avec la spécification de crédits `unlimited`. Par exemple, si vous redimensionnez une instance T3 en instance M4 alors qu'elle est en mode `unlimited`, Amazon EC2 renvoie l'instance M4.

```
aws ec2 describe-instance-credit-specifications --instance-id i-1234567890abcdef0
```

Exemple de sortie

```
{
  "InstanceCreditSpecifications": [
    {
      "InstanceId": "i-1234567890abcdef0",
      "CpuCredits": "unlimited"
    }
  ]
}
```

Modifier la spécification de crédits d'une instance de performance à capacité extensible

Vous pouvez changer la spécification de crédit d'une instance T en cours d'exécution ou arrêtée à tout moment entre `unlimited` et `standard`.

Veillez noter qu'en mode `unlimited`, une instance peut dépenser des crédits excédentaires, ce qui peut entraîner des frais supplémentaires. Pour plus d'informations, consultez [Les crédits excédentaires peuvent occasionner des frais](#).

Console

Pour modifier la spécification de crédit d'une instance T

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, choisissez Instances.
3. Sélectionnez l'instance. Pour modifier la spécification de crédits pour plusieurs instances à la fois, sélectionnez toutes les instances applicables.
4. Choisissez Actions, Instance settings (Paramètres de l'instance), Change credit specification (Modifier la spécification de crédits). Cette option n'est activée que si vous avez sélectionné une instance T.

5. Pour remplacer le mode de spécification de crédits par `unlimited`, activez la case à cocher en regard de l'ID de l'instance. Pour remplacer le mode de spécification de crédits par `standard`, désactivez la case à cocher en regard de l'ID de l'instance.

AWS CLI

Pour modifier la spécification de crédit d'une instance T

Utilisez la commande [modify-instance-credit-specification](#). Spécifiez l'instance et la spécification de crédits à l'aide du paramètre `--instance-credit-specification`. Les spécifications de crédits valides sont `unlimited` et `standard`.

```
aws ec2 modify-instance-credit-specification \
  --region us-east-1 \
  --instance-credit-specification
  "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

Exemple de sortie

```
{
  "SuccessfulInstanceCreditSpecifications": [
    {
      "InstanceId": "i- 1234567890abcdef0"
    }
  ],
  "UnsuccessfulInstanceCreditSpecifications": []
}
```

Définir la spécification de crédits par défaut pour le compte

Chaque famille d'instances T est fournie avec une [spécification de crédit par défaut](#). Vous pouvez modifier les spécifications de crédit par défaut pour chaque famille d'instances T au niveau du compte par AWS région.

Si vous utilisez l'assistant de lancement d'instance dans la console EC2 pour lancer des instances, la valeur que vous sélectionnez pour la spécification de crédits remplace celle par défaut au niveau du compte. Si vous utilisez le AWS CLI pour lancer des instances, toutes les nouvelles instances T du compte sont lancées en utilisant la spécification de crédit par défaut. La spécification de crédits pour les instances existantes en cours d'exécution ou arrêtées n'est pas affectée.

Considération

La spécification de crédits par défaut pour une famille d'instances ne peut être modifiée qu'une seule fois au cours d'une période continue de 5 minutes, et jusqu'à quatre fois au cours d'une période continue de 24 heures.

Console

Pour définir la spécification de crédits par défaut au niveau du compte par région

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation de gauche, sélectionnez EC2 Dashboard (Tableau de bord EC2).
4. Dans Account attributes (Attributs de compte), sélectionnez Default credit specification (Spécification de crédits par défaut).
5. Choisissez Gérer.
6. Pour chaque famille de l'instance, sélectionnez Unlimited (Illimité) ou Standard, puis sélectionnez Update (Mettre à jour).

AWS CLI

Pour définir la spécification de crédits par défaut au niveau du compte (AWS CLI)

Utilisez la commande [modify-default-credit-specification](#). Spécifiez la Région AWS , la famille d'instances et la spécification de crédits par défaut à l'aide du paramètre `--cpu-credits`. Les spécifications de crédits par défaut valides sont `unlimited` et `standard`.

```
aws ec2 modify-default-credit-specification \  
  --region us-east-1 \  
  --instance-family t2 \  
  --cpu-credits unlimited
```

Afficher la spécification de crédits par défaut

Vous pouvez consulter les spécifications de crédit par défaut d'une famille d'instances T au niveau du compte par AWS région.

Console

Pour consulter les spécifications de crédit par défaut au niveau du compte

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation de gauche, sélectionnez EC2 Dashboard (Tableau de bord EC2).
4. Dans Account attributes (Attributs de compte), sélectionnez Default credit specification (Spécification de crédits par défaut).

AWS CLI

Pour consulter les spécifications de crédit par défaut au niveau du compte

Utilisez la commande [get-default-credit-specification](#). Spécifiez la Région AWS et la famille d'instances.

```
aws ec2 get-default-credit-specification --region us-east-1 --instance-family t2
```

Surveiller vos crédits UC pour détecter les instances de performance à capacité extensible

EC2 envoie des métriques à Amazon CloudWatch. Vous pouvez consulter les mesures de crédit du processeur dans les mesures Amazon EC2 par instance de la CloudWatch console ou en utilisant le pour AWS CLI répertorier les mesures pour chaque instance. Pour plus d'informations, consultez [Répertorier les métriques à l'aide de la console](#) et [Listez les métriques à l'aide du AWS CLI](#).

Table des matières

- [CloudWatch Mesures supplémentaires pour les instances de performance éclatantes](#)
- [Calculer l'utilisation des crédits UC](#)

CloudWatch Mesures supplémentaires pour les instances de performance éclatantes

Les instances de performance Burstable disposent des CloudWatch indicateurs supplémentaires suivants, qui sont mis à jour toutes les cinq minutes :

- **CPUCreditUsage** – Nombre de crédits UC dépensés au cours de la période de mesure.
- **CPUCreditBalance** – Nombre de crédits UC qu'une instance a cumulés. Ce solde diminue lorsque les crédits UC sont dépensés plus rapidement qu'ils ne sont gagnés.
- **CPUSurplusCreditBalance** – Nombre de crédits UC excédentaires dépensés pour maintenir l'utilisation d'UC lorsque la métrique **CPUCreditBalance** est égale à zéro.
- **CPUSurplusCreditsCharged** – Nombre de crédits UC excédentaires qui dépassent le [nombre maximal de crédits UC](#) pouvant être gagnés en 24 heures, et qui génèrent donc des frais supplémentaires.

Les deux dernières métriques s'appliquent uniquement aux instances configurées en mode `unlimited`.

Le tableau suivant décrit les CloudWatch mesures relatives aux instances de performance en rafale. Pour plus d'informations, consultez [Répertoriez CloudWatch les métriques disponibles pour vos instances](#).

Métrique	Description
CPUCreditUsage	<p>Nombre de crédits UC dépensés par l'instance pour l'utilisation de l'UC. Par exemple, un crédit UC est équivalent à un processeur virtuel fonctionnant à 100 % d'utilisation pendant une minute ou une combinaison équivalente de processeurs virtuels, d'utilisation et de temps (par exemple, un processeur virtuel fonctionnant à 50 % d'utilisation pendant deux minutes, ou deux processeurs virtuels fonctionnant à 25 % d'utilisation pendant deux minutes).</p> <p>Les métriques de crédits UC sont disponibles uniquement toutes les 5 minutes. Si vous spécifiez une période supérieure à cinq minutes, utilisez la statistique <code>Sum</code> au lieu de la statistique <code>Average</code>.</p> <p>Unités : crédits (minutes vCPU)</p>
CPUCreditBalance	<p>Nombre de crédits UC gagnés qu'une instance a accumulés depuis son lancement ou son démarrage. Pour les instances T2</p>

Métrique	Description
	<p>Standard, le <code>CPUCreditBalance</code> inclut également le nombre de crédits de lancement qui ont été accumulés.</p> <p>Les crédits sont accumulés dans le solde de crédits quand ils sont gagnés et supprimés du solde de crédits lorsqu'ils sont dépensés. Le solde de crédits présente une limite maximum qui est déterminée par la taille de l'instance. Une fois que la limite est atteinte, tous les nouveaux crédits gagnés sont rejetés. Pour les instances T2 Standard, les crédits de lancement ne sont pas comptés dans la limite.</p> <p>L'instance peut dépenser les crédits figurant dans le <code>CPUCreditBalance</code> pour dépasser le niveau de base de l'utilisation de l'UC.</p> <p>Les crédits figurant dans le <code>CPUCreditBalance</code> d'une instance en cours d'exécution n'expirent pas. Lorsqu'une instance T4g, T3a ou T3 s'arrête, la <code>CPUCreditBalance</code> valeur persiste pendant sept jours. Au-delà, tous les crédits accumulés sont perdus. Lorsqu'une instance T2 s'arrête, la valeur de <code>CPUCreditBalance</code> n'est pas conservée, et tous les crédits accumulés sont perdus.</p> <p>Les métriques de crédits UC sont disponibles uniquement toutes les 5 minutes.</p> <p>Unités : crédits (minutes vCPU)</p>

Métrique	Description
CPUSurplusCreditBalance	<p>Nombre de crédits excédentaires ayant été dépensés par une instance <code>unlimited</code> lorsque la valeur <code>CPUCreditBalance</code> est nulle.</p> <p>La valeur de <code>CPUSurplusCreditBalance</code> est remboursé e progressivement par les crédits UC gagnés. Si le nombre de crédits excédentaires dépasse le nombre maximum de crédits que l'instance peut gagner en 24 heures, les crédits excédentaires dépensés au-dessus du maximum génèrent des frais supplémentaires.</p> <p>Unités : crédits (minutes vCPU)</p>
CPUSurplusCreditsCharged	<p>Nombre de crédits excédentaires dépensés qui ne sont pas remboursés progressivement par les crédits UC gagnés et qui génèrent donc des frais supplémentaires.</p> <p>Les crédits excédentaires dépensés sont facturés lorsque l'une des situations suivantes se produit :</p> <ul style="list-style-type: none"> • Les crédits excédentaires dépensés dépassent le nombre maximum de crédits que l'instance peut gagner sur une période de 24 heures. Les crédits excédentaires dépensés au-dessus de ce maximum sont facturés à la fin de l'heure. • L'instance est arrêtée ou résiliée. • L'instance bascule du mode <code>unlimited</code> au mode <code>standard</code>. <p>Unités : crédits (minutes vCPU)</p>

Calculer l'utilisation des crédits UC

L'utilisation du crédit CPU par les instances est calculée à l'aide CloudWatch des métriques d'instance décrites dans le tableau précédent.

Amazon EC2 envoie les métriques CloudWatch toutes les cinq minutes. Une référence à la valeur antérieure d'une métrique à un moment donné désigne la valeur précédente de cette métrique, envoyée 5 minutes auparavant.

Calculer l'utilisation des crédits UC pour les instances Standard

- Le solde de crédits UC augmente si l'utilisation de l'UC chute au-dessous du niveau de référence, lorsque les crédits dépensés sont inférieurs aux crédits gagnés au cours des cinq minutes précédentes.
- Le solde de crédits UC diminue si l'utilisation de l'UC est supérieure au niveau de référence, lorsque les crédits dépensés sont supérieurs aux crédits gagnés au cours des cinq minutes précédentes.

Cette description est illustrée d'un point de vue mathématique par l'équation suivante:

Exemple

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -  
CPUCreditUsage]
```

La taille de l'instance détermine le nombre de crédits que l'instance peut gagner par heure, ainsi que le nombre de crédits gagnés qu'elle peut accumuler dans le solde de crédits. Pour plus d'informations sur le nombre de crédits gagnés par heure et la limite du solde de crédits pour chaque taille d'instance, consultez le [tableau des crédits](#).

Exemple

Dans cet exemple, une instance t3.nano est utilisée. Pour calculer la valeur de CPUCreditBalance de l'instance, utilisez l'équation précédente comme suit :

- CPUCreditBalance – Solde de crédits actuel à calculer.
- prior CPUCreditBalance – Solde de crédits cinq minutes auparavant. Dans cet exemple, l'instance a accumulé deux crédits.
- Credits earned per hour – Une instance t3.nano gagne six crédits par heure.
- 5/60— Représente l'intervalle de cinq minutes entre la publication des CloudWatch métriques. Multipliez les crédits gagnés par heure par 5/60 (cinq minutes) pour obtenir le nombre de crédits gagnés par l'instance au cours des cinq dernières minutes. Une instance t3.nano gagne 0,5 crédits toutes les cinq minutes.

- `CPUCreditUsage` – Nombre de crédits dépensés par l'instance au cours des cinq dernières minutes. Dans cet exemple, l'instance a dépensé un crédit au cours des cinq dernières minutes.

Vous pouvez calculer la valeur du `CPUCreditBalance` à l'aide de ces valeurs :

Exemple

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Calculer l'utilisation des crédits UC pour les instances en mode Illimité

Lorsqu'une instance de performance à capacité extensible doit dépasser le niveau de base, elle dépense toujours ses crédits accumulés avant de dépenser les crédits excédentaires. Si elle épuise le solde de ses crédits UC accumulés, elle peut dépenser les crédits excédentaires pour une utilisation en mode rafale de l'UC aussi longtemps que nécessaire. Si l'utilisation de l'UC chute au-dessous du niveau de base, les crédits excédentaires sont toujours remboursés avant que l'instance n'accumule des crédits gagnés.

Nous employons le terme `Adjusted balance` dans les équations suivantes pour refléter l'activité qui se produit dans cet intervalle de cinq minutes. Nous utilisons cette valeur pour obtenir les valeurs des `CPUSurplusCreditBalance` CloudWatch métriques `CPUCreditBalance` et.

Exemple

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits earned per hour * (5/60) - CPUCreditUsage]
```

La valeur 0 du `Adjusted balance` indique que l'instance a dépensé l'ensemble de ses crédits gagnés pour une utilisation en mode rafale et qu'aucun crédit excédentaire n'a été dépensé. Le `CPUCreditBalance` et le `CPUSurplusCreditBalance` sont donc tous deux définis sur 0.

Une valeur positive pour le `Adjusted balance` indique que l'instance a accumulé des crédits gagnés, et que les crédits excédentaires précédents, le cas échéant, ont été remboursés. En conséquence, la valeur du `Adjusted balance` est attribuée au `CPUCreditBalance`, et le `CPUSurplusCreditBalance` est défini sur 0. La taille de l'instance détermine le [nombre maximal de crédits](#) qu'elle peut accumuler.

Exemple

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
```

```
CPUSurplusCreditBalance = 0
```

Une valeur négative pour le Adjusted balance indique que l'instance a dépensé tous les crédits gagnés qu'elle a accumulés, ainsi que des crédits excédentaires pour une utilisation en mode rafale. En conséquence, la valeur de Adjusted balance est attribuée à CPUSurplusCreditBalance et le CPUCreditBalance est défini sur 0. Là encore, la taille de l'instance détermine le [nombre maximal de crédits](#) qu'elle peut accumuler.

Exemple

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]  
CPUCreditBalance = 0
```

Si les crédits excédentaires dépensés dépassent le nombre maximal de crédits que l'instance peut accumuler, le solde de crédits excédentaires est défini sur le maximum, comme le montre l'équation précédente. Les crédits excédentaires restants représentés par la métrique CPUSurplusCreditsCharged sont facturés.

Exemple

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Pour finir, lorsque l'instance est résiliée, les crédits excédentaires suivis par le CPUSurplusCreditBalance sont facturés. Si l'instance bascule du mode unlimited au mode standard, tout solde CPUSurplusCreditBalance restant éventuel est également facturé.

Accélération des performances grâce aux instances de GPU

Les instances GPU donnent accès aux unités GPU NVIDIA avec des milliers de cœurs de calcul. Vous pouvez utiliser ces instances pour accélérer de nombreuses applications scientifiques, d'ingénierie et de rendu en tirant parti de l'architecture CUDA ou d'infrastructures de calcul parallèle OpenCL (Open Computing Language). Vous pouvez également les utiliser pour des applications graphiques, notamment les jeux en streaming, les applications 3D en streaming, et d'autres charges de travail graphiques.

Avant de pouvoir activer ou optimiser une instance basée sur un GPU, vous devez installer les pilotes appropriés, comme suit :

- Pour installer les pilotes NVIDIA sur une instance à laquelle est connecté un GPU NVIDIA, telle qu'une instance P3 ou G4dn, consultez. [Installer les pilotes NVIDIA](#)

- Pour installer les pilotes AMD sur une instance à laquelle est connecté un GPU AMD, telle qu'une instance G4ad, consultez. [Installer les pilotes AMD](#)

Table des matières

- [Activez les applications virtuelles NVIDIA GRID sur vos instances basées sur le GPU Amazon EC2](#)
- [Optimisation des paramètres GPU sur les instances Amazon EC2](#)
- [Configuration de deux écrans 4K sur les instances G4ad Linux](#)
- [Commencez avec les instances P5 pour Linux](#)

Activez les applications virtuelles NVIDIA GRID sur vos instances basées sur le GPU Amazon EC2

Pour activer les applications virtuelles GRID sur des instances basées sur un processeur graphique dotées de GPU NVIDIA (la station de travail virtuelle NVIDIA GRID est activée par défaut), vous devez définir le type de produit pour le pilote, comme suit.

Activer les applications virtuelles GRID sur les instances Linux

1. Créez le fichier `/etc/nvidia/gridd.conf` à partir du modèle de fichier fourni.

```
[ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
```

2. Ouvrez le fichier `/etc/nvidia/gridd.conf` dans votre éditeur de texte favori.
3. Trouvez la ligne `FeatureType` et affectez-lui la valeur `0`. Puis ajoutez une ligne avec `IgnoreSP=TRUE`.

```
FeatureType=0 IgnoreSP=TRUE
```

4. Enregistrez le fichier et quittez l'éditeur.
5. Redémarrez l'instance pour récupérer la nouvelle configuration.

```
[ec2-user ~]$ sudo reboot
```

Activer les applications virtuelles GRID sur les instances Windows

Activer les applications virtuelles GRID sur les instances Windows

1. Exécutez `regedit.exe` pour ouvrir l'éditeur de registre.
2. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global\GridLicensing`.
3. Ouvrez le menu contextuel (clic droit) et sélectionnez Nouveau, puis DWORD dans le volet de droite.
4. Dans Nom, entrez `FeatureType` et tapez `Enter`.
5. Ouvrez le menu contextuel (clic droit) `FeatureType` et choisissez Modifier.
6. Pour Données de la valeur, entrez `0` pour les applications virtuelles NVIDIA GRID et choisissez OK.
7. Ouvrez le menu contextuel (clic droit) et sélectionnez Nouveau, puis DWORD dans le volet de droite.
8. Pour Nom, saisissez `IgnoreSP`, puis tapez `Enter`.
9. Ouvrez le menu contextuel (clic droit) sur `IgnoreSP` et sélectionnez Modifier.
10. Pour Données de la valeur, tapez `1` et cliquez sur OK.
11. Fermez l'éditeur de registre.

Optimisation des paramètres GPU sur les instances Amazon EC2

Il existe plusieurs optimisations de configuration GPU que vous pouvez effectuer pour obtenir les meilleures performances sur les instances NVIDIA GPU. Avec certains de ces types d'instance, le pilote NVIDIA utilise une fonction `autoboost`, qui modifie les fréquences d'horloge GPU. En désactivant la fonction `autoboost` et en paramétrant les fréquences d'horloge GPU à leur fréquence maximale, vous pouvez obtenir les performances maximales de vos instances GPU.

Optimisation des paramètres du GPU sous Linux

1. Configurez les paramètres GPU de sorte qu'ils soient permanents. L'exécution de cette commande peut prendre plusieurs minutes.

```
[ec2-user ~]$ sudo nvidia-persistenced
```

2. [Instances G3 et P2 uniquement] Désactivez la fonction Autoboot pour tous les GPU de l'instance.

```
[ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
```

3. Définissez toutes les vitesses d'horloge GPU à leur fréquence maximale. Utilisez les vitesses d'horloge de mémoire et de graphiques spécifiées dans les commandes suivantes.

Certaines versions du pilote NVIDIA ne prennent pas en charge le réglage de la fréquence d'horloge de l'application et affichent l'erreur "Setting applications clocks is not supported for GPU...", que vous pouvez ignorer.

- instances G3 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
```

- instances G4dn :

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- Instances G5 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
```

- Instances G6 et Gr6 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
```

- instances P2 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- instances P3 et P3dn :

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- instances P4d :

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- Instances P4de :

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Instances P5 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Optimisation des paramètres du GPU sous Windows

1. Ouvrez une PowerShell fenêtre et accédez au dossier d'installation NVIDIA.

```
cd "C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\"
```

2. [Instances G3 et P2 uniquement] Désactivez la fonction Autoboot pour tous les GPU de l'instance.

```
.\nvidia-smi --auto-boost-default=0
```

3. Définissez toutes les vitesses d'horloge GPU à leur fréquence maximale. Utilisez les vitesses d'horloge de mémoire et de graphiques spécifiées dans les commandes suivantes.

Certaines versions du pilote NVIDIA ne prennent pas en charge le réglage de la fréquence d'horloge de l'application et affichent l'erreur "Setting applications clocks is not supported for GPU...", que vous pouvez ignorer.

- instances G3 :

```
.\nvidia-smi -ac "2505,1177"
```

- instances G4dn :

```
.\nvidia-smi -ac "5001,1590"
```

- Instances G5 :

```
.\nvidia-smi -ac "6250,1710"
```

- Instances G6 et Gr6 :

```
.\nvidia-smi -ac "6251,2040"
```

- instances P2 :

```
.\nvidia-smi -ac "2505,875"
```

- instances P3 et P3dn :

```
.\nvidia-smi -ac "877,1530"
```

- instances P4d :

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- Instances P4de :

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- Instances P5 :

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Configuration de deux écrans 4K sur les instances G4ad Linux

Lancer une instance G4ad

1. Connectez-vous à votre instance Linux pour obtenir l'adresse du bus PCI du GPU que vous voulez cibler pour le double 4K (2x4k) :

```
lspci -vv | grep -i amd
```

Vous obtenez une sortie similaire à ce qui suit :

```
00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev c3)  
Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
```

2. Notez que l'adresse du bus PCI est 00:1e.0 dans la sortie ci-dessus. Créez un fichier nommé /etc/modprobe.d/amdgpu.conf et ajoutez :

```
options amdgpu virtual_display=0000:00:1e.0,2
```

3. Pour installer les pilotes AMD sous Linux, voir [Installez les pilotes AMD sur votre instance Amazon EC2](#). Si vous avez déjà installé le pilote GPU AMD, vous devrez recréer les modules du noyau amdgpu via dkms.
4. Utilisez le fichier xorg.conf ci-dessous pour définir la topologie de l'écran double (2x4K) et enregistrez le fichier dans /etc/X11/xorg.conf :

```
~$ cat /etc/X11/xorg.conf
Section "ServerLayout"
    Identifier      "Layout0"
    Screen          0 "Screen0"
    Screen          1 "Screen1"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
    Option          "Xinerama" "1"
EndSection
Section "Files"
    ModulePath      "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath      "/opt/amdgpu/lib/xorg/modules"
    ModulePath      "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath      "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath      "/usr/lib64/xorg/modules"
    ModulePath      "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier      "Mouse0"
    Driver          "mouse"
    Option          "Protocol" "auto"
    Option          "Device" "/dev/psaux"
    Option          "Emulate3Buttons" "no"
    Option          "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier      "Keyboard0"
    Driver          "kbd"
EndSection

Section "Monitor"
```

```
    Identifier    "Virtual"
    VendorName    "Unknown"
    ModelName     "Unknown"
    Option        "Primary" "true"
EndSection

Section "Monitor"
    Identifier    "Virtual-1"
    VendorName    "Unknown"
    ModelName     "Unknown"
    Option        "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier    "Device0"
    Driver        "amdgpu"
    VendorName    "AMD"
    BoardName     "Radeon MxGPU V520"
    BusID         "PCI:0:30:0"
EndSection

Section "Device"
    Identifier    "Device1"
    Driver        "amdgpu"
    VendorName    "AMD"
    BoardName     "Radeon MxGPU V520"
    BusID         "PCI:0:30:0"
EndSection

Section "Extensions"
    Option        "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier    "Screen0"
    Device        "Device0"
    Monitor       "Virtual"
    DefaultDepth  24
    Option        "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

```

Section "Screen"
    Identifier      "Screen1"
    Device          "Device1"
    Monitor         "Virtual"
    DefaultDepth    24
    Option          "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual      3840 2160
        Depth        32
    EndSubSection
EndSection

```

5. Configurez DCV en suivant les instructions de la configuration d'un [bureau interactif](#).
6. Une fois la configuration de DCV terminée, redémarrez.
7. Confirmez que le pilote est fonctionnel :

```
dmesg | grep amdgpu
```

Les résultats doivent avoir l'aspect suivant :

```
Initialized amdgpu
```

8. Vous devriez voir dans la sortie pour `DISPLAY=:0 xrandr -q` que vous avez 2 écrans virtuels connectés :

```

~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
 0mm x 0mm
4096x3112  60.00
3656x2664  59.99
4096x2160  60.00
3840x2160  60.00
1920x1200  59.95
1920x1080  60.00
1600x1200  59.95
1680x1050  60.00
1400x1050  60.00
1280x1024  59.95
1440x900   59.99
1280x960   59.99

```

```

1280x854 59.95
1280x800 59.96
1280x720 59.97
1152x768 59.95
1024x768 60.00 59.95
800x600 60.32 59.96 56.25
848x480 60.00 59.94
720x480 59.94
640x480 59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
0mm
4096x3112 60.00
3656x2664 59.99
4096x2160 60.00
3840x2160 60.00
1920x1200 59.95
1920x1080 60.00
1600x1200 59.95
1680x1050 60.00
1400x1050 60.00
1280x1024 59.95
1440x900 59.99
1280x960 59.99
1280x854 59.95
1280x800 59.96
1280x720 59.97
1152x768 59.95
1024x768 60.00 59.95
800x600 60.32 59.96 56.25
848x480 60.00 59.94
720x480 59.94
640x480 59.94 59.94

```

9. Lorsque vous vous connectez à DCV, changez la résolution à 2x4K, confirmant que le support double écran est enregistré par DCV.



```

3840x2160 @0x0 - Display 1
3840x2160 @3840x0 - Display 2

```

Commencez avec les instances P5 pour Linux

Les instances P5 fournissent 8 GPU NVIDIA H100 avec 640 Go de mémoire GPU à bande passante élevée. Elles sont équipées de processeurs AMD EPYC de 3e génération et fournissent 2 To de mémoire système, 30 To de stockage d'instance NVMe local, une bande passante du réseau agrégée de 3 200 Gbit/s et la prise en charge de GPUDirect RDMA. Les instances P5 prennent également en charge la technologie Amazon UltraCluster EC2, qui permet de réduire la latence et d'améliorer les performances du réseau grâce à l'EFA.

Le tableau suivant présente un résumé des spécifications p5.48xlarge.

vCPU	Mémoire système	GPU	Mémo GPU	Bande passante réseau	GPUDirect RDMA	GPU pair à pair	Stockage d'instances
192	2 Tio	8 processeurs graphiques NVIDIA H100	HBM3 640 Go	3 200 Gbit/s avec EFAv2	Pris en charge	NVSw 900 GIs	8 volumes SSD NVMe de 3 800 Go

Configuration logicielle :

Le moyen le plus simple de démarrer avec les instances P5 est de lancer une instance à l'aide d'un [AWS Deep Learning AMI](#) qui est préconfiguré avec tous les logiciels requis. Pour connaître les dernières AWS Deep Learning AMI versions à utiliser avec les instances P5, consultez l'[AMI GPU AWS Deep Learning Base \(Ubuntu 20.04\)](#).

Si vous devez créer une AMI personnalisée à utiliser avec des instances P5, nous vous recommandons d'installer les versions logicielles minimales suivantes :

- Pilote NVIDIA 535.54.03 ou version ultérieure
- CUDA 12.1 ou version ultérieure
- NVIDIA GDRCopy 2.3 ou version ultérieure
- Programme d'installation EFA 1.24.1 ou version ultérieure
- NCCL 2.18.3 ou version ultérieure
- aws-ofi-nccl plugin 1.7.2-aws ou version ultérieure

Nous vous recommandons également de configurer l'instance de façon à ne pas utiliser d'états C plus profonds. Pour plus d'informations, consultez la section [Performances élevées et faible latence en limitant les états C plus profonds](#) dans le guide de l'utilisateur Amazon Linux 2. La dernière AMI GPU AWS Deep Learning Base est préconfigurée pour ne pas utiliser d'états C plus profonds.

Recommandations spécifiques à Ubuntu 20.04

Les recommandations suivantes pour Ubuntu 20.04 permettent d'éviter les noms d'interface imprévisibles au démarrage :

- Assurez-vous que vous utilisez `systemd 245.4-4ubuntu3.19` ou une version ultérieure en exécutant la commande suivante :

```
systemd --version
```

- Assurez-vous d'avoir configuré GRUB :
 - Ouvrez le fichier de configuration `/etc/default/grub` dans un éditeur de texte.
 - Modifiez l'entrée `GRUB_CMDLINE_LINUX_DEFAULT` pour l'inclure `net.naming-scheme=v247`.
 - Redémarrez votre instance en exécutant `sudo update-grub`.

Configuration du réseau et de l'EFA

Les instances P5 fournissent 3 200 Gbit/s de bande passante du réseau en utilisant plusieurs interfaces EFA. Les instances P5 prennent en charge 32 cartes réseau. Nous vous recommandons de définir une seule interface réseau EFA par carte réseau. Pour configurer ces interfaces au lancement, nous vous recommandons d'utiliser les paramètres suivants :

- Pour l'interface réseau 0, spécifiez l'index d'appareils 0.
- Pour les interfaces réseaux 1 à 31, spécifiez l'index d'appareils 1.

Pour plus d'informations sur la manière de configurer de vos instances P5 pour EFA, consultez [Commencer à utiliser les instances P5 et EFA](#).

instances Mac Amazon EC2

Les instances Amazon EC2 Mac prennent en charge le système d'exploitation macOS de manière native.

- Les instances EC2 Mac (mac1.meta1) basées sur x86 sont construites sur du matériel 2018 Mac mini alimenté par des processeurs Core i7 Intel de huitième génération (Coffee Lake) de 3,2 GHz.
- Les instances EC2 M1 Mac (mac2.meta1) sont construites sur du matériel 2020 Mac mini alimenté par des processeurs Apple Silicon M1.
- Les instances EC2 M2 Mac (mac2-m2.meta1) sont construites sur du matériel 2023 Mac mini alimenté par des processeurs Apple Silicon M2.
- Les instances EC2 M2 Pro Mac (mac2-m2pro.meta1) sont construites sur du matériel 2023 Mac mini alimenté par des processeurs Apple Silicon M2 Pro.

Les instances EC2 Mac sont idéales pour développer, construire, tester et signer des applications pour les plateformes Apple, telles que les iPhone, iPad, iPod, Mac, Vision Pro, Apple Watch, Apple TV et Safari. Vous pouvez vous connecter à votre instance Mac en utilisant SSH ou Apple Remote Desktop (ARD).

 Note

L'unité de facturation est l'hôte dédié. Les instances exécutées sur cet hôte n'engendrent pas de frais supplémentaires.

Table des matières

- [Considérations](#)
- [Préparation de l'instance](#)
- [AMI macOS EC2](#)
- [EC2 macOS Init](#)
- [Moniteur système Amazon EC2 pour macOS](#)
- [Ressources connexes](#)
- [Lancer une instance Mac](#)
- [Connexion à votre instance Mac](#)
- [Mettre à jour le système d'exploitation et le logiciel sur les instances Mac](#)
- [Augmenter la taille d'un volume EBS sur votre instance Mac](#)
- [Arrêt ou résiliation de votre instance Mac](#)
- [Trouvez les versions de macOS prises en charge pour votre hôte dédié Amazon EC2 Mac](#)

- [S'abonner aux notifications d'image AMI macOS](#)
- [Notes de mise à jour des AMI macOS Amazon EC2](#)

Considérations

Les considérations suivantes s'appliquent aux instances Mac :

- Les instances Mac ne sont disponibles qu'en tant qu'instances à matériel nu sur [Hôtes dédiés](#), avec une période d'allocation minimale de 24 heures avant de pouvoir libérer l'Hôte dédié. Vous pouvez lancer une instance Mac par Hôte dédié. Vous pouvez partager l'hôte dédié avec les AWS comptes ou les unités organisationnelles de votre AWS organisation, ou avec l'ensemble de AWS l'organisation.
- Les instances Mac sont disponibles en différentes versions Régions AWS. Pour obtenir une liste de la disponibilité des instances Mac dans chacune des régions Régions AWS, consultez la section [Types d'instances Amazon EC2 par région](#).
- Les instances Mac ne sont disponibles qu'en tant que instances à la demande. Ils ne sont pas disponibles en tant que instances Spot ou instances réservées. Vous pouvez effectuer des économies sur les instances Mac en souscrivant à un [Savings Plan](#).
- Les instances Mac peuvent exécuter l'un des systèmes d'exploitation suivants :
 - macOS Mojave (version 10.14) (instances Mac basées sur x86 uniquement)
 - macOS Catalina (version 10.15) (instances Mac basées sur x86 uniquement)
 - macOS Big Sur (version 11) (instances Mac basées sur x86 et M1)
 - macOS Monterey (version 12) (instances Mac basées sur x86 et M1)
 - macOS Ventura (version 13) (toutes les instances Mac, instances M2 et Mac M2 Pro compatibles avec macOS Ventura version 13.2 ou ultérieure)
 - macOS Sonoma (version 14) (toutes les instances Mac)
- EBSle hotplug est pris en charge.
- AWS ne gère ni ne prend en charge le SSD interne du matériel Apple. Nous vous recommandons vivement d'utiliser plutôt des volumes Amazon EBS. EBSles volumes offrent les mêmes avantages en termes d'élasticité, de disponibilité et de durabilité sur les instances Mac que sur toute autre instance EC2.
- Nous recommandons d'utiliser un SSD à usage général (gp2etgp3) et un SSD IOPS provisionné (io1etio2) avec des instances Mac pour des performances optimalesEBS.
- [Les instances Mac prennent en charge Amazon EC2 Auto Scaling](#).

- Sur les instances Mac basées sur x86, les mises à jour logicielles automatiques sont désactivées. Nous vous recommandons d'appliquer les mises à jour et de les tester sur votre instance avant de mettre l'instance en production. Pour plus d'informations, consultez [Mettre à jour le système d'exploitation et le logiciel sur les instances Mac](#).
- Lorsque vous arrêtez ou résiliez une instance Mac, un workflow de nettoyage est effectué sur Hôte dédié. Pour plus d'informations, consultez [Arrêt ou résiliation de votre instance Mac](#).

Warning

Ne pas utiliser FileVault. L'activation FileVault empêchera le démarrage de l'hôte en raison du verrouillage des partitions. Si le chiffrement des données est requis, utilisez le chiffrement Amazon EBS pour éviter les problèmes de démarrage et l'impact sur les performances. Avec le chiffrement Amazon EBS, les opérations de chiffrement sont effectuées sur les serveurs hébergeant les instances, garantissant ainsi la sécurité à la fois data-in-transit entre une instance data-at-rest et le stockage EBS qui lui est rattaché. Pour plus d'informations, consultez la section relative au [chiffrement Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS

Préparation de l'instance

Après avoir lancé une instance Mac, vous devez attendre qu'elle soit prête avant de pouvoir vous y connecter. Pour une AMI AWS vendue avec une instance Mac x86 ou une instance Apple Silicon Mac, le temps de lancement peut aller d'environ 6 minutes à 20 minutes. Le temps de lancement peut augmenter en fonction de la taille des volumes Amazon EBS choisis, de l'inclusion de scripts supplémentaires dans les données utilisateur ou du chargement des logiciels supplémentaires sur une AMI macOS personnalisée.

Vous pouvez utiliser un petit script shell, comme celui ci-dessous, pour interroger l' `describe-instance-status` API afin de savoir quand l'instance est prête à être connectée. Dans la commande suivante, remplacez l'exemple d'ID d'instance par le vôtre.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-ids=i-0123456789example \
  --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

AMI macOS EC2

macOS Amazon EC2 est conçu pour fournir un environnement stable, sécurisé et hautes performances pour les charges de travail des développeurs exécutées sur des instances Mac Amazon EC2. Les AMI macOS EC2 incluent des packages permettant une intégration facile AWS, tels que des outils de configuration de lancement et des AWS bibliothèques et outils populaires.

Pour plus d'informations sur les AMI EC2 macOS, consultez [Notes de mise à jour des AMI macOS Amazon EC2](#).

AWS fournit régulièrement des AMI EC2 macOS mises à jour, notamment des mises à jour des packages appartenant à macOS AWS et de la dernière version entièrement testée de macOS. En outre, AWS fournit des AMI mises à jour avec les dernières mises à jour de versions mineures ou majeures dès qu'elles ont été testées et vérifiées. Si vous n'avez pas besoin de conserver les données ou les personnalisations de vos instances Mac, vous pouvez obtenir les dernières mises à jour en lançant une nouvelle instance à l'aide de l'AMI actuelle et résilier l'instance précédente. Sinon, vous pouvez choisir les mises à jour à appliquer à vos instances Mac.

Pour plus d'informations sur la façon de s'abonner aux notifications AMI macOS, consultez [S'abonner aux notifications d'image AMI macOS](#).

EC2 macOS Init

EC2macOS Init est utilisé pour initialiser les instances EC2 Mac au lancement. Il utilise des groupes de priorités pour exécuter des groupes logiques de tâches en même temps.

Le fichier launchd plist est `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. Les fichiers pour EC2 macOS Init se trouvent dans `/usr/local/aws/ec2-macos-init`.

Pour plus d'informations, consultez <https://github.com/aws/ec2-macos-init>.

Moniteur système Amazon EC2 pour macOS

Amazon EC2 System Monitor pour macOS fournit des indicateurs d'utilisation du processeur à Amazon CloudWatch. Il envoie ces métriques à CloudWatch un périphérique série personnalisé par périodes d'une minute. Vous pouvez activer ou désactiver cet agent comme suit. Il est activé par défaut.

```
sudo setup-ec2monitoring [enable | disable]
```

Note

Amazon EC2 System Monitor pour macOS n'est actuellement pas pris en charge sur les instances Apple Silicon Mac.

Ressources connexes

Pour plus d'informations sur la tarification, consultez [Tarification](#).

Pour plus d'informations sur les instances Mac, consultez [Instances Amazon EC2 Mac](#).

Pour plus d'informations sur les spécifications matérielles et les performances réseau des instances Mac, consultez la section [Instances à usage général](#).

Lancer une instance Mac

Les instances EC2 Mac nécessitent un [hôte dédié](#). Vous devez d'abord attribuer un hôte à votre compte, puis lancer l'instance sur cet hôte.

Vous pouvez lancer une instance Mac à l'aide du AWS Management Console ou du AWS CLI.

Lancer une instance Mac à l'aide de la console

Pour lancer une instance Mac sur un Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Allouez l'hôte dédié, comme suit :
 - a. Dans le volet de navigation, choisissez Hôtes dédiés.
 - b. Choisissez Allouer Hôte dédié, puis procédez comme suit :
 - i. Pour Famille d'instances, choisissez mac1, mac2, mac2-m2 ou mac2-m2pro. Si la famille de l'instance n'apparaît pas dans la liste, elle n'est pas prise en charge dans la région actuellement sélectionnée.
 - ii. Pour Type d'instance, choisissez mac1.metal, mac2.metal, mac2-m2.metal ou mac2-m2pro.metal en fonction de la famille d'instances choisie.
 - iii. Pour Zone de disponibilité, choisissez la zone de disponibilité pour votre Hôte dédié.
 - iv. Pour Quantity (Quantité), conservez 1.

- v. Choisissez Allouer.
3. Lancez l'instance sur l'hôte, comme suit :
 - a. Sélectionnez le Hôte dédié que vous avez créé, puis procédez comme suit :
 - i. Choisissez Actions, puis Launch instance(s) onto host (Lancer les instances sur l'hôte).
 - ii. Sous Application and OS Images (Amazon Machine Image) (Images d'applications et de systèmes d'exploitation (Amazon Machine Image)), sélectionnez une AMI macOS.
 - iii. Sous Type d'instance, sélectionnez le type d'instance approprié (mac1.metal, mac2.metal, mac2-m2.metal ou mac2-m2pro.metal).
 - iv. Sous Advanced details (Détails avancés), vérifiez que les paramètres Tenancy (Location), Tenancy host by (Hôte de location par) et Tenancy host ID (ID d'hôte de location) sont préconfigurés en fonction de l'hôte dédié que vous avez créé. Mettez à jour la valeur Tenancy affinity (Affinité de location), si nécessaire.
 - v. Terminez les étapes de l'assistant en spécifiant les volumes EBS, les groupes de sécurité et les paires de clés selon les besoins.
 - vi. Dans le panneau Summary (Récapitulatif), sélectionnez Launch instance (Lancer l'instance).
 - b. Une page de confirmation indique que l'instance est en cours de lancement. Sélectionnez View all instances (Afficher toutes les instances) pour fermer la page de confirmation et revenir à la console. L'état initial d'une instance est pending. L'instance est prête lorsque son état passe à running et qu'elle passe avec succès les vérifications de statut.

Lancez une instance Mac à l'aide du AWS CLI

Allouer l'hôte dédié

Utilisez la commande [allocate-hosts](#) suivante pour allouer un hôte dédié à votre instance Mac, en remplaçant le `instance-type` par `mac1.metal`, `mac2.metal`, `mac2-m2.metal` ou `mac2-m2pro.metal`, et la `region` et la `availability-zone` par celles appropriées à votre environnement.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-zone us-east-1b --auto-placement "on" --quantity 1
```

Lancer l'instance sur l'hôte

Utilisez la commande [run-instances](#) suivante pour lancer une instance Mac, en remplaçant à nouveau le `instance-type` par `mac1.metal`, `mac2.metal`, `mac2-m2.metal` ou `mac2-m2pro.metal`, et la `region` et la `availability-zone` par celles utilisées précédemment.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement  
Tenancy=host --image-id ami_id --key-name my-key-pair
```

L'état initial d'une instance est `pending`. L'instance est prête lorsque son état passe à `running` et qu'elle passe avec succès les vérifications de statut. Utilisez la commande [describe-instance-status](#) suivante pour afficher les informations de statut de votre instance.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Voici un exemple de sortie pour une instance qui est en cours d'exécution et qui a passé avec succès les contrôles de statut.

```
{  
  "InstanceStatuses": [  
    {  
      "AvailabilityZone": "us-east-1b",  
      "InstanceId": "i-017f8354e2dc69c4f",  
      "InstanceState": {  
        "Code": 16,  
        "Name": "running"  
      },  
      "InstanceState": {  
        "Details": [  
          {  
            "Name": "reachability",  
            "Status": "passed"  
          }  
        ],  
        "Status": "ok"  
      },  
      "SystemStatus": {  
        "Details": [  
          {  
            "Name": "reachability",  
            "Status": "passed"  
          }  
        ],  
        "Status": "ok"  
      }  
    }  
  ]  
}
```

```
}  
  }  
] }  
}
```

Connexion à votre instance Mac

Vous pouvez vous connecter à votre instance Mac à l'aide du protocole SSH ou d'une interface utilisateur graphique.

Se connecter à votre instance à l'aide de SSH

Important

Plusieurs utilisateurs peuvent accéder simultanément au système d'exploitation. Généralement, il existe une session user:GUI 1:1 en raison du service intégré de partage d'écran sur le port 5900. L'utilisation de SSH dans macOS prend en charge plusieurs sessions jusqu'à la limite « Max Sessions » dans le fichier `sshd_config`.

Les instances Mac Amazon EC2 n'autorisent pas les connexions à distance avec le SSH racine par défaut. De plus, l'authentification par mot de passe est désactivée pour empêcher les attaques de force sur les mots de passe. Le compte `ec2-user` est configuré pour se connecter à distance à l'aide de SSH. Le compte `ec2-user` dispose également de privilèges `sudo`. Une fois que vous vous êtes connecté à votre instance, vous pouvez ajouter d'autres utilisateurs.

Pour prendre en charge la connexion à votre instance à l'aide de SSH, lancez l'instance à l'aide d'une paire de clés et d'un groupe de sécurité qui autorise l'accès SSH, et assurez-vous que l'instance dispose d'une connectivité Internet. Vous fournissez le fichier `.pem` de la paire de clés lorsque vous vous connectez à l'instance.

Utilisez la procédure suivante pour vous connecter à votre instance Mac à l'aide d'un client SSH. Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [Résoudre les problèmes de connexion à votre instance Linux](#).

Pour vous connecter à votre instance à l'aide de SSH

1. Vérifiez que votre ordinateur local dispose d'un client SSH en entrant `ssh` sur la ligne de commande. Si votre ordinateur ne reconnaît pas la commande, recherchez un client SSH pour votre système d'exploitation et installez-le.

2. Obtenir le nom de serveur DNS public de votre instance Dans la console Amazon EC2, vous pouvez trouver le nom DNS public dans les onglets Détails et Mise en réseau . À l'aide de AWS CLI, vous pouvez trouver le nom DNS public à l'aide de la commande [describe-instances](#).
3. Recherchez le fichier .pem pour la paire de clés que vous avez spécifiée lorsque vous avez lancé l'instance.
4. Connectez-vous à votre instance à l'aide de la commande ssh suivante, en spécifiant le nom DNS public de l'instance et le fichier .pem.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

Connexion à l'interface utilisateur graphique (GUI) de votre instance

Utilisez la procédure suivante pour vous connecter à l'interface utilisateur graphique de votre instance à l'aide de VNC, d'Apple Remote Desktop (ARD) ou de l'application de partage d'écran Apple (incluse dans macOS).

Note

macOS 10.14 et les versions ultérieures ne permettent le contrôle que si le partage d'écran est activé via [Préférences système](#).

Pour vous connecter à votre instance à l'aide du client ARD ou du client VNC

1. Vérifiez qu'un client ARD ou qu'un client VNC prenant en charge ARD est installé sur votre ordinateur local. Sur macOS, vous pouvez utiliser l'application Partage d'écran intégrée. Sinon, recherchez ARD pour votre système d'exploitation et installez-le.
2. À partir de votre ordinateur local, [connectez-vous à votre instance à l'aide de SSH](#).
3. Configurez un mot de passe pour le compte ec2-user à l'aide de la commande passwd comme suit.

```
[ec2-user ~]$ sudo passwd ec2-user
```

4. Installez et exécutez le partage d'écran macOS à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
```

```
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

5. Déconnectez-vous votre instance en saisissant `exit` et en appuyant sur la touche Entrée.
6. À partir de votre ordinateur, connectez-vous à votre instance à l'aide de la commande `ssh` suivante. Outre les options indiquées dans la section précédente, utilisez l'option `-L` pour activer le transfert de port et transférer tout le trafic sur le port local 5900 vers le serveur ARD de l'instance.

```
ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

7. À partir de votre ordinateur local, utilisez le client ARD ou le client VNC prenant en charge ARD pour vous connecter à `localhost:5900`. Par exemple, utilisez l'application Partage d'écran sur macOS comme suit :
 - a. Ouvrez le Finder et sélectionnez Aller.
 - b. Sélectionnez Se connecter au serveur.
 - c. Dans le champ Adresse du serveur, saisissez `vnc://localhost:5900`.
 - d. Connectez-vous à l'invite, en utilisant **ec2-user** comme nom d'utilisateur et le mot de passe que vous avez créés pour le compte `ec2-user`.

Modifier la résolution d'écran macOS sur les instances Mac

Une fois connecté à votre instance Mac EC2 à l'aide d'ARD ou d'un client VNC prenant en charge la version ARD, vous pouvez modifier la résolution d'écran de votre environnement macOS à l'aide de l'un des outils ou utilitaires macOS disponibles publiquement, tels que [displayplacer](#).

Pour modifier la résolution d'écran à l'aide de `displayplacer`

1. Installez `displayplacer`.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Affichez les informations actuelles sur l'écran et les résolutions d'écran possibles.

```
[ec2-user ~]$ displayplacer list
```

3. Appliquez la résolution d'écran souhaitée.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
degree:0"
```

Par exemple :

```
RES="2560x1600"
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
origin:(0,0) degree:0"
```

Mettre à jour le système d'exploitation et le logiciel sur les instances Mac

Warning

L'installation des versions bêta ou préliminaire de macOS n'est disponible que sur les instances Mac M1 Amazon EC2. Amazon EC2 ne qualifie pas les versions bêta ou préliminaire de macOS et ne garantit pas que les instances resteront fonctionnelles après la mise à jour d'une version de pré-production de macOS.

Toute tentative d'installation des versions bêta ou préliminaires de macOS sur des instances Mac x86 Amazon EC2 entraînera la dégradation de votre hôte dédié Mac Amazon EC2 lorsque vous arrêtez ou résiliez vos instances, et vous empêchera de démarrer ou de lancer une nouvelle instance sur cet hôte.

Étapes de mise à jour du logiciel sur les instances Mac x86 et les instances Apple Silicon Mac.

- [Mettre à jour le logiciel sur les instances Mac x86](#)
- [Mettre à jour le logiciel sur les instances Apple Silicon Mac](#)

Mettre à jour le logiciel sur les instances Mac x86

Sur les instances Mac basées sur x86, vous pouvez installer les mises à jour du système d'exploitation d'Apple à l'aide de la commande `softwareupdate`.

Pour installer les mises à jour du système d'exploitation d'Apple sur des instances Mac basées sur x86

1. Répertoriez les packages avec des mises à jour disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ softwareupdate --list
```

2. Installez toutes les mises à jour ou uniquement des mises à jour spécifiques. Pour installer des mises à jour spécifiques, utilisez la commande suivante.

```
[ec2-user ~]$ sudo softwareupdate --install label
```

Pour installer toutes les mises à jour, utilisez la commande suivante.

```
[ec2-user ~]$ sudo softwareupdate --install --all --restart
```

Les administrateurs système peuvent utiliser AWS Systems Manager pour déployer des mises à jour préapprouvées du système d'exploitation sur des instances Mac x86. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Systems Manager](#).

Vous pouvez utiliser Homebrew pour installer des mises à jour des packages dans les AMI EC2 macOS, afin de disposer de la dernière version de ces packages sur vos instances. Vous pouvez également utiliser Homebrew pour installer et exécuter des applications macOS courantes sur macOS Amazon EC2. Pour plus d'informations, consultez la [documentation Homebrew](#).

Pour installer des mises à jour en utilisant Homebrew

1. Mettez à jour Homebrew en utilisant la commande suivante.

```
[ec2-user ~]$ brew update
```

2. Répertoriez les packages avec des mises à jour disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ brew outdated
```

3. Installez toutes les mises à jour ou uniquement des mises à jour spécifiques. Pour installer des mises à jour spécifiques, utilisez la commande suivante.

```
[ec2-user ~]$ brew upgrade package name
```

Pour installer toutes les mises à jour, utilisez la commande suivante.

```
[ec2-user ~]$ brew upgrade
```

Mettre à jour le logiciel sur les instances Apple Silicon Mac

Considérations

Pilote de l'Adaptateur réseau élastique (ENA)

En raison d'une mise à jour de la configuration du pilote réseau, la version 1.0.2 du pilote ENA n'est pas compatible avec macOS 13.3 ou toute autre version ultérieure. Si vous voulez installer une version 13.3 ou ultérieure bêta, préliminaire ou de production de macOS et que vous n'avez pas installé le dernier pilote ENA, suivez la procédure suivante pour installer une nouvelle version du pilote.

Pour installer une nouvelle version du pilote ENA

1. Dans une fenêtre du terminal, connectez-vous à votre instance Apple Silicon Mac à l'aide de [SSH](#).
2. Téléchargez l'application ENA dans le fichier Applications à l'aide de la commande suivante.

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

Conseil pour la résolution de problèmes

Si vous recevez l'avertissement `No available formula with the name amazon-ena-ethernet-dext`, exécutez la commande suivante.

```
[ec2-user ~]$ brew update
```

3. Déconnectez-vous votre instance en saisissant `exit` et en appuyant sur la touche Retour.
4. Utilisez le client VNC pour activer l'application ENA.
 - a. Configurez le client VNC en utilisant [Connexion à l'interface utilisateur graphique \(GUI\) de votre instance](#).

- b. Une fois connecté à votre instance à l'aide de l'application de partage d'écran, accédez au dossier Applications et ouvrez l'application ENA.
- c. Choisissez Activer
- d. Pour vérifier que le pilote a été correctement activé, exécutez la commande suivante dans la fenêtre du terminal. La sortie de la commande indique que l'ancien pilote est arrêté et que le nouveau pilote est activé.

```
systemextensionsctl list;
```

- e. Une fois l'instance redémarrée, seul le nouveau pilote est présent.

Mise à jour du logiciel sur les instances Apple Silicon Mac

Sur les instances Apple Silicon Mac, vous devez effectuer plusieurs étapes pour procéder à une mise à jour du système d'exploitation sur place. Tout d'abord, accédez au disque interne de l'instance à l'aide de l'interface graphique avec un client VNC (Virtual Network Computing). Cette procédure utilise le partage d'écran macOS, le client VNC intégré. Déléguez ensuite la propriété à l'utilisateur administratif (`ec2-user`) en vous connectant en tant qu'`aws-managed-user` sur le volume Amazon EBS.

Au cours de cette procédure, vous créez deux mots de passe. Un mot de passe est destiné à l'utilisateur administratif (`ec2-user`) et l'autre est destiné à un utilisateur administratif spécial (`aws-managed-user`). N'oubliez pas ces mots de passe, car vous les utiliserez tout au long de la procédure.

Note

Avec cette procédure sur macOS Big Sur, vous ne pouvez effectuer que des mises à jour mineures, telles que la mise à jour de macOS Big Sur 11.7.3 vers macOS Big Sur 11.7.4. Pour macOS Monterey ou version ultérieure, vous pouvez effectuer des mises à jour logicielles majeures.

Accès au disque interne

1. Depuis votre ordinateur local, dans le terminal, connectez-vous à votre instance Apple Silicon Mac via le protocole SSH à l'aide de la commande suivante. Pour plus d'informations, consultez [Se connecter à votre instance à l'aide de SSH](#).

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

2. Installez et exécutez le partage d'écran macOS à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing  
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

3. Définissez un mot de passe pour `ec2-user` à l'aide de la commande suivante. N'oubliez pas le mot de passe, car vous l'utiliserez plus tard.

```
[ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
```

4. Déconnectez-vous de l'instance en saisissant `exit` et en appuyant sur la touche Retour.
5. Depuis votre ordinateur local, dans le terminal, reconnectez-vous à votre instance avec un tunnel SSH vers le port VNC à l'aide de la commande suivante.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-dns-name
```

Note

Ne quittez pas cette session SSH tant que les étapes suivantes de connexion VNC et d'interface graphique ne sont pas terminées. Lorsque l'instance est redémarrée, la connexion se ferme automatiquement.

6. À partir de votre ordinateur local, connectez-vous à `localhost:5900` en suivant les étapes ci-après :
 - a. Ouvrez le Finder et sélectionnez Aller.
 - b. Sélectionnez Se connecter au serveur.
 - c. Dans le champ Adresse du serveur, saisissez `vnc://localhost:5900`.

7. Dans la fenêtre macOS, connectez-vous à la session distante de l'instance Apple Silicon Mac en tant qu'`ec2-user` à l'aide du mot de passe que vous avez créé à l'[étape 3](#).
8. Accédez au disque interne, nommé `InternalDisk`, à l'aide de l'une des options suivantes.
 - a. Pour macOS Ventura ou version ultérieure : ouvrez Réglages Système, sélectionnez Général dans le volet gauche, puis Disque de démarrage en bas à droite du volet.
 - b. Pour macOS Monterey ou version antérieure : ouvrez les Préférences Système, sélectionnez Disque de démarrage, puis déverrouillez le volet en cliquant sur l'icône de verrouillage en bas à gauche de la fenêtre.

 Conseil pour la résolution de problèmes

Si vous devez monter le disque interne, exécutez la commande suivante dans le terminal.

```
APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep  
"Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;  
diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
```

9. Choisissez le disque interne, nommé `InternalDisk`, puis sélectionnez Redémarrer. Sélectionnez Redémarrer à nouveau lorsque vous y êtes invité.

 Important

Si le disque interne est nommé Macintosh HD au lieu de `InternalDisk`, votre instance doit être arrêtée et redémarrée afin que l'hôte dédié puisse être mis à jour. Pour plus d'informations, consultez [Arrêt ou résiliation de votre instance Mac](#).

Utilisez la procédure suivante pour déléguer la propriété à l'utilisateur administratif. Lorsque vous vous reconnectez à votre instance via SSH, vous démarrez à partir du disque interne à l'aide de l'utilisateur administratif spécial (`aws-managed-user`). Le mot de passe initial de `aws-managed-user` est vide, vous devez donc le remplacer lors de votre première connexion. Ensuite, répétez les étapes d'installation et de démarrage du partage d'écran macOS, car le volume de démarrage a changé.

Délégation de la propriété à l'administrateur sur un volume Amazon EBS

1. Depuis votre ordinateur local, dans le terminal, connectez-vous à votre instance Apple Silicon Mac à l'aide de la commande suivante.

```
ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
```

2. Lorsque vous recevez l'avertissement `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`, exécutez l'une des commandes suivantes pour résoudre le problème.
 - a. Supprimez les hôtes connus à l'aide de la commande suivante. Ensuite, répétez l'étape précédente.

```
rm ~/.ssh/known_hosts
```

- b. Ajoutez ce qui suit à la commande SSH de l'étape précédente.

```
-o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
```

3. Définissez le mot de passe pour `aws-managed-user` à l'aide de la commande suivante. Le mot de passe initial `aws-managed-user` est vide, vous devez donc le remplacer lors de votre première connexion.

- a.

```
[aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-user password
```

- b. Lorsque vous recevez le message `Permission denied. Please enter user's old password:`, appuyez sur Entrée.

Conseil pour la résolution de problèmes

Si l'erreur `passwd: DS error: eDSAuthFailed` s'affiche, utilisez la commande suivante.

```
[aws-managed-user ~]$ sudo passwd aws-managed-user
```

4. Installez et exécutez le partage d'écran macOS à l'aide de la commande suivante.

```
[aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
```

```
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

5. Déconnectez-vous de l'instance en saisissant `exit` et en appuyant sur la touche Retour.
6. Depuis votre ordinateur local, dans le terminal, reconnectez-vous à votre instance avec un tunnel SSH vers le port VNC à l'aide de la commande suivante.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-public-dns-name
```

7. À partir de votre ordinateur local, connectez-vous à `localhost:5900` en suivant les étapes ci-après :
 - a. Ouvrez le Finder et sélectionnez Aller.
 - b. Sélectionnez Se connecter au serveur.
 - c. Dans le champ Adresse du serveur, saisissez `vnc://localhost:5900`.
8. Dans la fenêtre macOS, connectez-vous à la session distante de l'instance Apple Silicon Mac en tant qu'`aws-managed-user` à l'aide du mot de passe que vous avez créé à l'[étape 3](#).

Note

Si un message vous invite à vous connecter avec votre identifiant Apple, sélectionnez Configurer plus tard.

9. Accédez au volume Amazon EBS à l'aide de l'une des options suivantes.
 - a. Pour macOS Ventura ou version ultérieure : ouvrez Réglages Système, sélectionnez Général dans le volet gauche, puis Disque de démarrage en bas à droite du volet.
 - b. Pour macOS Monterey ou version antérieure : ouvrez les Préférences Système, sélectionnez Disque de démarrage, puis déverrouillez le volet à l'aide de l'icône de verrouillage en bas à gauche de la fenêtre.

Note

En attendant le redémarrage, lorsqu'un message vous invite à saisir un mot de passe administrateur, utilisez celui que vous avez défini ci-dessus pour `aws-managed-user`. Ce mot de passe peut être différent de celui que vous avez défini pour `ec2-user` ou le

compte administrateur par défaut de votre instance. Les instructions suivantes indiquent quand utiliser le mot de passe administrateur de votre instance.

10. Sélectionnez le volume Amazon EBS (le volume non nommé InternalDisk dans la fenêtre du disque de démarrage) et choisissez Redémarrer.

Note

Si plusieurs volumes Amazon EBS démarrables sont attachés à votre instance Apple Silicon Mac, veillez à utiliser un nom unique pour chaque volume.

11. Confirmez le redémarrage, puis choisissez Autoriser les utilisateurs lorsqu'un message vous y invite.
12. Dans le volet Autoriser l'utilisateur sur ce volume, vérifiez que l'utilisateur administratif (ec2-user par défaut) est sélectionné, puis sélectionnez Autoriser.
13. Saisissez le mot de passe ec2-user que vous avez créé à l'[étape 3](#) de la procédure précédente, puis sélectionnez Continuer.
14. Saisissez le mot de passe de l'utilisateur administratif spécial (aws-managed-user) lorsqu'un message vous y invite.
15. À partir de votre ordinateur local, dans le terminal, reconnectez-vous à votre instance à l'aide de SSH et du nom d'utilisateur ec2-user.

Conseil pour la résolution de problèmes

Si l'avertissement WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! s'affiche, exécutez la commande suivante et reconnectez-vous à votre instance via SSH.

```
rm ~/.ssh/known_hosts
```

16. Pour effectuer la mise à jour logicielle, utilisez les commandes sous [Mettre à jour le logiciel sur les instances Mac x86](#).

Augmenter la taille d'un volume EBS sur votre instance Mac

Vous pouvez augmenter la taille de vos volumes Amazon EBS sur votre instance Mac. Pour plus d'informations, consultez [Amazon EBS Elastic Volumes](#) dans le guide de l'utilisateur Amazon EBS.

Après avoir augmenté la taille du volume, vous devez augmenter la taille de votre conteneur APFS comme suit.

Augmentez l'espace disque disponible à l'utilisation

1. Déterminez si un redémarrage est requis. Si vous redimensionnez un volume EBS existant sur une instance Mac en cours d'exécution, vous devez [redémarrer](#) l'instance pour rendre la nouvelle taille disponible. Si la modification de l'espace disque a été effectuée pendant le lancement, le redémarrage n'est pas requis.

Affichez l'état actuel des tailles de disque :

```
[ec2-user ~]$ diskutil list external physical
/dev/disk0 (external, physical):
#:                TYPE NAME                SIZE          IDENTIFIER
0:                GUID_partition_scheme      *322.1 GB     disk0
1:                EFI EFI                209.7 MB     disk0s1
2:                Apple_APFS Container disk2    321.9 GB     disk0s2
```

2. Copiez et collez la commande suivante.

```
[ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -d" " -f8)
yes | sudo diskutil repairDisk $PDISK
```

3. Copiez et collez la commande suivante.

```
[ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
```

Arrêt ou résiliation de votre instance Mac

Lorsque vous arrêtez une instance Mac, l'instance reste dans l'état `stopping` pendant environ 15 minutes avant de passer à l'état `stopped`.

Lorsque vous arrêtez ou résiliez une instance Mac, Amazon EC2 effectue un workflow de nettoyage sur l'hôte dédié sous-jacent pour effacer le SSD interne, supprimer les variables NVRAM persistantes et mettre à jour le dernier firmware de l'appareil. Cela garantit que les instances Mac offrent la même sécurité et la même confidentialité des données que les autres instances EC2 Nitro. Il vous permet également d'exécuter les dernières AML macOS. Lors du workflow de nettoyage, l'hôte dédié entre

temporairement dans l'état en attente. Sur les instances Mac basées sur x86, le flux de travail de nettoyage peut prendre jusqu'à 50 minutes. Sur les instances Apple Silicon Mac, le flux de travail de nettoyage peut prendre jusqu'à 110 minutes. En outre, sur les instances Mac basées sur x86, si le firmware de l'appareil doit être mis à jour, le flux de travail de nettoyage peut prendre jusqu'à 3 heures.

Vous ne pouvez pas démarrer l'instance Mac arrêtée ou lancer une nouvelle instance Mac avant la fin du workflow de nettoyage, moment où Hôte dédié entre dans l'état `available`.

La mesure et la facturation sont suspendues lorsque l'hôte dédié entre dans l'état `pending`. Vous n'êtes pas facturé pour la durée du workflow de nettoyage.

Libérez l'Hôte dédié pour votre instance Mac

Lorsque vous avez terminé avec votre instance Mac, vous pouvez libérer l'Hôte dédié. Avant de pouvoir libérer l'Hôte dédié, vous devez arrêter ou résilier l'instance Mac. Vous ne pouvez pas libérer l'hôte tant que la période d'allocation n'excède pas le minimum de 24 heures.

Pour libérer l'Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et État de l'instance, puis sélectionnez Arrêter l'instance ou Résilier l'instance.
4. Dans le volet de navigation, choisissez Hôtes dédiés.
5. Sélectionnez Hôte dédié puis Actions, Libérer l'hôte.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Release (Libérer).

Trouvez les versions de macOS prises en charge pour votre hôte dédié Amazon EC2 Mac

Vous pouvez consulter les dernières versions de macOS prises en charge par votre hôte Amazon EC2 Mac Dedicated Host. Grâce à cette fonctionnalité, vous pouvez vérifier si votre hôte dédié peut prendre en charge les lancements d'instances avec vos versions préférées de macOS.

Chaque version de macOS nécessite une version minimale du microprogramme sur le Mac Apple sous-jacent pour démarrer correctement. La version du microprogramme Apple Mac peut devenir

obsolète si un hôte dédié Mac alloué est resté inactif pendant une période prolongée ou s'il contient une instance de longue date.

Pour garantir la compatibilité avec les dernières versions de macOS, vous pouvez arrêter ou résilier des instances sur l'hôte dédié Mac qui vous a été attribué. Cela déclenche le flux de travail de nettoyage de l'hôte et met à jour le microprogramme du Mac Apple sous-jacent pour qu'il soit compatible avec les dernières versions de macOS. Un hôte dédié doté d'une instance de longue durée sera automatiquement mis à jour lorsque vous arrêtez ou mettez fin à une instance en cours d'exécution.

Pour plus d'informations sur le flux de travail de nettoyage, consultez [Arrêt ou résiliation de votre instance Mac](#).

Pour plus d'informations sur le lancement d'instances Mac, consultez [Lancer une instance Mac](#).

Vous pouvez consulter les informations relatives aux dernières versions de macOS prises en charge sur l'hôte dédié qui vous a été attribué à l'aide de la console Amazon EC2 ou du AWS CLI

Console

Pour afficher les informations relatives au microprogramme de l'hôte dédié à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sur la page de détails des hôtes dédiés, sous Dernières versions de macOS prises en charge, vous pouvez voir les dernières versions de macOS prises en charge par l'hôte.

AWS CLI

Pour consulter les informations relatives au microprogramme de l'hôte dédié à l'aide du AWS CLI

Utilisez la [describe-mac-hosts](#) commande en la région remplaçant par la commande appropriée Région AWS.

```
$ aws ec2 describe-mac-hosts --region us-east-1
{
  "MacHosts": [
    {
      "HostId": "h-07879acf49EXAMPLE",
      "MacOSLatestSupportedVersions": [
        "14.3",
```

```
        "13.6.4",  
        "12.7.3"  
    ]  
  }  
]  
}
```

S'abonner aux notifications d'image AMI macOS

Pour être informé quand de nouvelles images AMI sont publiées ou quand BridGeOS a été mis à jour, abonnez-vous aux notifications via Amazon SNS.

Pour plus d'informations sur les AMI macOS EC2, consultez [Notes de mise à jour des AMI macOS Amazon EC2](#).

Pour vous abonner aux notifications d'image AMI macOS

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez utiliser cette région, car les notifications SNS auxquelles vous vous abonnez ont été créées dans cette région.
3. Dans le panneau de navigation, choisissez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, procédez comme suit :
 - a. Pour Topic ARN (ARN de la rubrique), copiez et collez l'un des Amazon Resource Names (ARN) suivants :
 - **arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates**
 - **arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates**
 - b. Pour Protocole, sélectionnez l'une des options suivantes :
 - E-mail :

Pour Endpoint (Point de terminaison), tapez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications. Une fois votre abonnement créé, vous recevrez un message de confirmation avec la ligne d'objet AWS Notification - Subscription

Confirmation. Ouvrez l'e-mail et choisissez Confirm subscription (Confirmer l'abonnement) pour terminer votre abonnement.

- SMS :

Pour Endpoint (Point de terminaison), tapez un numéro de téléphone que vous pouvez utiliser pour recevoir les notifications.

- AWS Lambda, Amazon SQS, Amazon Data Firehose (les notifications sont au format JSON) :

Pour Point de terminaison, entrez l'ARN de la fonction Lambda, la file d'attente SQS ou le flux Firehose que vous pouvez utiliser pour recevoir les notifications.

c. Choisissez Create subscription (Créer un abonnement).

Chaque fois que des images AMI macOS sont publiées, nous envoyons des notifications aux abonnés de la rubrique `amazon-ec2-macos-ami-updates`. A chaque mise à jour de brifgeOS, nous envoyons des notifications aux abonnés de la rubrique `amazon-ec2-bridgeos-updates`. Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Pour vous désabonner des notifications d'image AMI macOS

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez utiliser cette région, car les notifications SNS ont été créées dans cette région.
3. Dans le panneau de navigation, choisissez Abonnements.
4. Sélectionnez les abonnements, puis choisissez Actions, Delete subscriptions (Supprimer les abonnements). Lorsque vous êtes invité à confirmer, choisissez Delete (Supprimer).

Notes de mise à jour des AMI macOS Amazon EC2

Les informations suivantes fournissent des informations détaillées sur les packages inclus par défaut dans les AMI EC2 macOS et résumant les modifications apportées à chaque version des AMI EC2 macOS.

Pour plus d'informations sur la façon de s'abonner aux notifications AMI macOS, consultez [S'abonner aux notifications d'image AMI macOS](#).

Packages par défaut inclus dans les AMI macOS Amazon EC2

Le tableau suivant décrit les packages inclus par défaut dans les AMI macOS EC2.

Packages	Notes de mise à jour
EC2macOS Init	https://github.com/aws/ec2-macos-init/tags
EC2Utilitaires pour macOS	https://github.com/aws/ec2-macos-utils/tags
AmazonAgent SSM	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI) version 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Outils de ligne de commande pour Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
EC2 Instance Connect	https://github.com/aws/aws-ec2-instance-connect-config/releases
Safari	https://developer.apple.com/documentation/safari-release-notes

Mises à jour de l'AMI macOS Amazon EC2

Le tableau suivant décrit les modifications incluses dans les versions de l'AMI macOS EC2. Notez que certaines modifications s'appliquent à toutes les AMI macOS EC2, tandis que d'autres ne s'appliquent qu'à un sous-ensemble de ces AMI.

Mises à jour de l'AMI macOS EC2

Version	Modifications
2024,06.07	Toutes les AMI <ul style="list-style-type: none"> • Homebrew mis à jour vers la version 4.3.1-1

Version	Modifications
	<ul style="list-style-type: none">• Mise à jour <code>aws-cli</code> au format 2.15.56• Mis à jour <code>amazon-ssm-agent</code> au code 3.3.380.0-1 <p>Sortie de macOS Sonoma 14.5 (toutes les instances Mac)</p> <ul style="list-style-type: none">• Consignes de sécurité de macOS Sonoma 14.5 <p>Sortie de macOS Ventura 13.6.7 (toutes les instances Mac)</p> <ul style="list-style-type: none">• Consignes de sécurité de macOS Ventura 13.6.7• Safari mis à jour vers la version 17.5<ul style="list-style-type: none">• Consignes de sécurité de Safari 17.5 <p>Sortie de macOS Monterey 12.7.5 (toutes les instances Mac)</p> <ul style="list-style-type: none">• Consignes de sécurité de macOS Monterey 12.7.5• Safari mis à jour vers la version 17.5<ul style="list-style-type: none">• Consignes de sécurité de Safari 17.5

Version	Modifications
2024,04.12	<p>Toutes les AMI</p> <ul style="list-style-type: none">• Homebrew mis à jour vers la version 4.2.16-1• Mise à jour <code>aws-cli</code> au format 2.15.36 <p>Sortie de macOS Sonoma 14.4.1 (toutes les instances Mac)</p> <ul style="list-style-type: none">• Consignes de sécurité de macOS Sonoma 14.4.1 <p>Sortie de macOS Ventura 13.6.6 (toutes les instances Mac)</p> <ul style="list-style-type: none">• Consignes de sécurité de macOS Ventura 13.6.6• Safari mis à jour vers la version 17.4.1<ul style="list-style-type: none">• Consignes de sécurité de Safari 17.4.1 <p>Pour macOS Monterey (toutes les instances Mac)</p> <ul style="list-style-type: none">• Safari mis à jour vers la version 17.4.1<ul style="list-style-type: none">• Consignes de sécurité de Safari 17.4.1

instances optimisées pour Amazon EBS

Une instance optimisée pour Amazon EBS utilise une pile de configuration optimisée et fournit une capacité supplémentaire dédiée aux I/O Amazon EBS. Cette optimisation offre les meilleures performances pour vos volumes EBS en réduisant les conflits entre les I/O Amazon EBS et le trafic restant de votre instance.

Les instances optimisées par EBS fournissent une bande passante dédiée vers Amazon EBS. Lorsqu'ils sont attachés à une instance optimisée pour EBS, les volumes SSD polyvalents (gp2 et gp3) sont conçus pour garantir au moins 90 % de leurs performances d'IOPS provisionnés, et ce 99 % du temps au cours d'une année donnée, et les volumes SSD à IOPS provisionnées (io1 et io2) sont conçus pour garantir au moins 90 % de leurs performances provisionnées, et ce 99,9 % du temps au cours d'une année donnée. Les volumes HDD à débit optimisé (st1) et les volumes HDD à froid (sc1) garantissent tous deux au moins 90 % de leurs performances de débit prévues, et ce

99 % du temps au cours d'une année donnée. Les périodes non conformes sont assez uniformément réparties, en ciblant 99 % du débit total attendu chaque heure. Pour plus d'informations, consultez les [types de volumes Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Important

Les performances EBS d'une instance sont limitées par les limites de performances de l'instance ou par les performances agrégées de ses volumes attachés, la plus petite de ces valeurs s'appliquant. Pour atteindre des performances EBS optimales, une instance doit être attachée à des volumes offrant des performances combinées égales ou supérieures aux performances maximales de l'instance. Par exemple, pour atteindre 80,000 IOPS pour `r6i.16xlarge`, l'instance doit avoir au moins 5 volumes gp3, chacun alloués avec 16,000 IOPS (5 volumes x 16,000 IOPS = 80,000 IOPS).

Table des matières

- [Types d'instance pris en charge](#)
- [Obtenir les performances maximales](#)
- [Afficher les types d'instances qui prennent en charge l'optimisation EBS](#)
- [Activer l'optimisation EBS au lancement](#)
- [Activer l'optimisation EBS pour une instance existante](#)

Types d'instance pris en charge

Les tableaux suivants présentent les types d'instance qui prennent en charge l'optimisation pour EBS. Ils comprennent la bande passante dédiée à Amazon EBS, le débit agrégé maximum type qui peut être atteint sur cette connexion avec une charge de travail de streaming et une taille d'I/O de 128 Kio, ainsi que le nombre maximal d'IOPS que l'instance peut prendre en charge si vous utilisez une taille d'I/O de 16 Kio.

Choisissez une instance optimisée pour EBS qui fournit un débit Amazon EBS dédié supérieur aux besoins de votre application. Sinon, la connexion entre Amazon EBS et Amazon EC2 peut devenir un goulot d'étranglement des performances.

Table des matières

- [Optimisée pour EBS par défaut](#)

- [Optimisation EBS prise en charge](#)

Optimisée pour EBS par défaut

Le tableau suivant présente les types d'instance qui prennent en charge l'optimisation EBS par défaut et pour lesquels cette optimisation est activée par défaut. Il n'y a aucune nécessité d'activer l'optimisation EBS. Désactiver celle-ci n'a aucun effet.

Note

Vous pouvez également consulter ces informations par programme à l'aide du AWS CLI. Pour plus d'informations, consultez [Afficher les types d'instances qui prennent en charge l'optimisation EBS](#).

Rubriques

- [Usage général](#)
- [Calcul optimisé](#)
- [Optimisé pour la mémoire](#)
- [Stockage optimisé](#)
- [Calcul accéléré](#)
- [Calcul haute performance](#)

Usage général

Important

¹ Ces instances peuvent prendre en charge des performances maximales pendant 30 minutes au moins une fois toutes les 24 heures, délai au-delà duquel elles reviennent à leurs performances de base.

² Ces instances peuvent maintenir leurs performances déclarées indéfiniment. Si votre charge de travail nécessite des performances maximales soutenues pendant plus de 30 minutes, utilisez l'une de ces instances.

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
a1.medium ¹	300	3500	37,50	437,50	2500	20 000
a1.large ¹	525	3500	65,62	437,50	4000	20 000
a1.xlarge ¹	800	3500	100,00	437,50	6 000	20 000
a1.2xlarge ¹	1750	3500	218,75	437,50	10 000	20 000
a1.4xlarge ²		3500		437,5		20 000
a1.metal ²		3500		437,5		20 000
m4.large ²		450		56,25		3600
m4.xlarge ²		750		93,75		6 000
m4.2xlarge ²		1 000		125,0		8000
m4.4xlarge ²		2000		250,0		16000
m4.10xlarge ²		4000		500,0		32000
m4.16xlarge ²		10 000		1250,0		65000
m5.large ¹	650	4750	81,25	593,75	3600	18750
m5.xlarge ¹	1150	4750	143,75	593,75	6 000	18750

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m5.2xlarge ₁	2300	4750	287,50	593,75	12 000	18750
m5.4xlarge ₂		4750		593,75		18750
m5.8xlarge ₂		6800		850,0		30 000
m5.12xlarge ₂		9500		1187,5		40 000
m5.16xlarge ₂		13600		1700,0		60000
m5.24xlarge ₂		19000		2375,0		80000
m5.metal ²		19000		2375,0		80000
m5a.large ₁	650	2880	81,25	360,00	3600	16000
m5a.xlarge ₁	1085	2880	135,62	360,00	6 000	16000
m5a.2xlarge ₁	1580	2880	197,50	360,00	8333	16000
m5a.4xlarge ₂		2880		360,0		16000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m5a.8xlarge ²		4750		593,75		20 000
m5a.12xlarge ²		6780		847,5		30 000
m5a.16xlarge ²		9500		1187,5		40 000
m5a.24xlarge ²		13750		1718,75		60000
m5ad.large ¹	650	2880	81,25	360,00	3600	16000
m5ad.xlarge ¹	1085	2880	135,62	360,00	6 000	16000
m5ad.2xlarge ¹	1580	2880	197,50	360,00	8333	16000
m5ad.4xlarge ²		2880		360,0		16000
m5ad.8xlarge ²		4750		593,75		20 000
m5ad.12xlarge ²		6780		847,5		30 000
m5ad.16xlarge ²		9500		1187,5		40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m5ad.24xlarge ²		13750		1718,75		60000
m5d.large ¹	650	4750	81,25	593,75	3600	18750
m5d.xlarge ¹	1150	4750	143,75	593,75	6 000	18750
m5d.2xlarge ¹	2300	4750	287,50	593,75	12 000	18750
m5d.4xlarge ²		4750		593,75		18750
m5d.8xlarge ²		6800		850,0		30 000
m5d.12xlarge ²		9500		1187,5		40 000
m5d.16xlarge ²		13600		1700,0		60000
m5d.24xlarge ²		19000		2375,0		80000
m5d.metal ²		19000		2375,0		80000
m5dn.large ¹	650	4750	81,25	593,75	3600	18750

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m5dn.xlarge ¹	1150	4750	143,75	593,75	6 000	18750
m5dn.2xlarge ¹	2300	4750	287,50	593,75	12 000	18750
m5dn.4xlarge ²		4750		593,75		18750
m5dn.8xlarge ²		6800		850,0		30 000
m5dn.12xlarge ²		9500		1187,5		40 000
m5dn.16xlarge ²		13600		1700,0		60000
m5dn.24xlarge ²		19000		2375,0		80000
m5dn.metad ²		19000		2375,0		80000
m5n.large ¹	650	4750	81,25	593,75	3600	18750
m5n.xlarge ¹	1150	4750	143,75	593,75	6 000	18750
m5n.2xlarge ¹	2300	4750	287,50	593,75	12 000	18750

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m5n.4xlarge ²	4750		593,75		18750	
m5n.8xlarge ²	6800		850,0		30 000	
m5n.12xlarge ²	9500		1187,5		40 000	
m5n.16xlarge ²	13600		1700,0		60000	
m5n.24xlarge ²	19000		2375,0		80000	
m5n.metal ²	19000		2375,0		80000	
m5zn.large ¹	800	3170	100,00	396,25	3333	13333
m5zn.xlarge ¹	1564	3170	195,50	396,25	6667	13333
m5zn.2xlarge ²	3170		396,25		13333	
m5zn.3xlarge ²	4750		593,75		20 000	
m5zn.6xlarge ²	9500		1187,5		40 000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m5zn.12xlarge ²	19000			2375,0		80000
m5zn.medium ²	19000			2375,0		80000
m6a.large ¹	650	10 000	81,25	1250,00	3600	40 000
m6a.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
m6a.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
m6a.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
m6a.8xlarge ²	10 000			1250,0		40 000
m6a.12xlarge ²	15000			1875,0		60000
m6a.16xlarge ²	20 000			2500,0		80000
m6a.24xlarge ²	30 000			3750,0		120000
m6a.32xlarge ²	40 000			5000,0		160000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m6a.48xlarge ²	40 000			5000,0		240000
m6a.metal ²	40 000			5000,0		240000
m6g.medium ¹	315	4750	39,38	593,75	2500	20 000
m6g.large ¹	630	4750	78,75	593,75	3600	20 000
m6g.xlarge ¹	1188	4750	148,50	593,75	6 000	20 000
m6g.2xlarge ¹	2375	4750	296,88	593,75	12 000	20 000
m6g.4xlarge ²	4750			593,75		20 000
m6g.8xlarge ²	9500			1187,5		40 000
m6g.12xlarge ²	14250			1781,25		50000
m6g.16xlarge ²	19000			2375,0		80000
m6g.metal ²	19000			2375,0		80000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m6gd.medium ¹	315	4750	39,38	593,75	2500	20 000
m6gd.large ¹	630	4750	78,75	593,75	3600	20 000
m6gd.xlarge ¹	1188	4750	148,50	593,75	6 000	20 000
m6gd.2xlarge ¹	2375	4750	296,88	593,75	12 000	20 000
m6gd.4xlarge ²		4750		593,75		20 000
m6gd.8xlarge ²		9500		1187,5		40 000
m6gd.12xlarge ²		14250		1781,25		50000
m6gd.16xlarge ²		19000		2375,0		80000
m6gd.metal ²		19000		2375,0		80000
m6i.large ¹	650	10 000	81,25	1250,00	3600	40 000
m6i.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m6i.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
m6i.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
m6i.8xlarge ²		10 000		1250,0		40 000
m6i.12xlarge ²		15000		1875,0		60000
m6i.16xlarge ²		20 000		2500,0		80000
m6i.24xlarge ²		30 000		3750,0		120000
m6i.32xlarge ²		40 000		5000,0		160000
m6i.metal ²		40 000		5000,0		160000
m6id.large ¹	650	10 000	81,25	1250,00	3600	40 000
m6id.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
m6id.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m6id.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
m6id.8xlarge ²		10 000		1250,0		40 000
m6id.12xlarge ²		15000		1875,0		60000
m6id.16xlarge ²		20 000		2500,0		80000
m6id.24xlarge ²		30 000		3750,0		120000
m6id.32xlarge ²		40 000		5000,0		160000
m6id.metall ²		40 000		5000,0		160000
m6idn.large ¹	1562	25000	195,31	3125,00	6250	100 000
m6idn.xlarge ¹	3125	25000	390,62	3125,00	12500	100 000
m6idn.2xlarge ¹	6250	25000	781,25	3125,00	25000	100 000
m6idn.4xlarge ¹	12500	25000	1562,50	3125,00	50000	100 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m6idn.8xlarge ²	25000			3125,0		100 000
m6idn.12xlarge ²	37500			4687,5		150000
m6idn.16xlarge ²	50000			6250,0		200 000
m6idn.24xlarge ²	75000			9375,0		300 000
m6idn.32xlarge ²	100 000			12500,0		400 000
m6idn.metal ²	100 000			12500,0		400 000
m6in.large ¹	1562	25000	195,31	3125,00	6250	100 000
m6in.xlarge ¹	3125	25000	390,62	3125,00	12500	100 000
m6in.2xlarge ¹	6250	25000	781,25	3125,00	25000	100 000
m6in.4xlarge ¹	12500	25000	1562,50	3125,00	50000	100 000
m6in.8xlarge ²	25000			3125,0		100 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m6in.12xlarge ²	37500			4687,5		150000
m6in.16xlarge ²	50000			6250,0		200 000
m6in.24xlarge ²	75000			9375,0		300 000
m6in.32xlarge ²	100 000			12500,0		400 000
m6in.meta1 ²	100 000			12500,0		400 000
m7a.medium ¹	325	10 000	40,62	1250,00	2500	40 000
m7a.large ¹	650	10 000	81,25	1250,00	3600	40 000
m7a.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
m7a.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
m7a.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
m7a.8xlarge ²	10 000			1250,0		40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m7a.12xlarge ²		15000		1875,0		60000
m7a.16xlarge ²		20 000		2500,0		80000
m7a.24xlarge ²		30 000		3750,0		120000
m7a.32xlarge ²		40 000		5000,0		160000
m7a.48xlarge ²		40 000		5000,0		240000
m7a.metal-48xl ²		40 000		5000,0		240000
m7g.medium ¹	315	10 000	39,38	1250,00	2500	40 000
m7g.large ¹	630	10 000	78,75	1250,00	3600	40 000
m7g.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
m7g.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
m7g.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m7g.8xlarge ²		10 000		1250,0		40 000
m7g.12xlarge ²		15000		1875,0		60000
m7g.16xlarge ²		20 000		2500,0		80000
m7g.metal ²		20 000		2500,0		80000
m7gd.medium ¹	315	10 000	39,38	1250,00	2500	40 000
m7gd.large ¹	630	10 000	78,75	1250,00	3600	40 000
m7gd.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
m7gd.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
m7gd.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
m7gd.8xlarge ²		10 000		1250,0		40 000
m7gd.12xlarge ²		15000		1875,0		60000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m7gd.16xlarge ²	20 000			2500,0		80000
m7gd.metal 2	20 000			2500,0		80000
m7i.large ¹	650	10 000	81,25	1250,00	3600	40 000
m7i.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
m7i.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
m7i.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
m7i.8xlarge ²	10 000			1250,0		40 000
m7i.12xlarge ²	15000			1875,0		60000
m7i.16xlarge ²	20 000			2500,0		80000
m7i.24xlarge ²	30 000			3750,0		120000
m7i.48xlarge ²	40 000			5000,0		240000
m7i.metal-24xl ²	30 000			3750,0		120000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
m7i.metal-48xl ²		40 000		5000,0		240000
m7i-flex.large ¹	312	10 000	39,06	1250,00	2500	40 000
m7i-flex.xlarge ¹	625	10 000	78,12	1250,00	3600	40 000
m7i-flex.2xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
m7i-flex.4xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
m7i-flex.8xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
mac1.meta ²		14000		1750,0		80000
mac2.meta ²		10 000		1250,0		55000
mac2-m2.metal ²		8000		1000,0		55000
mac2-m2pro.metal ²		8000		1000,0		55000
t3.nano ¹	43	2085	5,38	260,62	250	11800
t3.micro ¹	87	2085	10,88	260,62	500	11800

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
t3.small ¹	174	2085	21,75	260,62	1 000	11800
t3.medium ¹	347	2085	43,38	260,62	2000	11800
t3.large ¹	695	2780	86,88	347,50	4000	15700
t3.xlarge ¹	695	2780	86,88	347,50	4000	15700
t3.2xlarge ¹	695	2780	86,88	347,50	4000	15700
t3a.nano ¹	45	2085	5,62	260,62	250	11800
t3a.micro ¹	90	2085	11,25	260,62	500	11800
t3a.small ¹	175	2085	21,88	260,62	1 000	11800
t3a.medium ¹	350	2085	43,75	260,62	2000	11800
t3a.large ¹	695	2780	86,88	347,50	4000	15700
t3a.xlarge ¹	695	2780	86,88	347,50	4000	15700
t3a.2xlarge ¹	695	2780	86,88	347,50	4000	15700
t4g.nano ¹	43	2085	5,38	260,62	250	11800
t4g.micro ¹	87	2085	10,88	260,62	500	11800
t4g.small ¹	174	2085	21,75	260,62	1 000	11800
t4g.medium ¹	347	2085	43,38	260,62	2000	11800

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
t4g.large ¹	695	2780	86,88	347,50	4000	15700
t4g.xlarge ¹	695	2780	86,88	347,50	4000	15700
t4g.2xlarge ¹	695	2780	86,88	347,50	4000	15700

Calcul optimisé

Important

¹ Ces instances peuvent prendre en charge des performances maximales pendant 30 minutes au moins une fois toutes les 24 heures, délai au-delà duquel elles reviennent à leurs performances de base.

² Ces instances peuvent maintenir leurs performances déclarées indéfiniment. Si votre charge de travail nécessite des performances maximales soutenues pendant plus de 30 minutes, utilisez l'une de ces instances.

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c4.large ²		500		62,5		4000
c4.xlarge ²		750		93,75		6 000
c4.2xlarge ²		1 000		125,0		8000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c4.4xlarge ₂	2000		250,0		16000	
c4.8xlarge ₂	4000		500,0		32000	
c5.large ¹	650	4750	81,25	593,75	4000	20 000
c5.xlarge ¹	1150	4750	143,75	593,75	6 000	20 000
c5.2xlarge ₁	2300	4750	287,50	593,75	10 000	20 000
c5.4xlarge ₂	4750		593,75		20 000	
c5.9xlarge ₂	9500		1187,5		40 000	
c5.12xlarge ₂	9500		1187,5		40 000	
c5.18xlarge ₂	19000		2375,0		80000	
c5.24xlarge ₂	19000		2375,0		80000	
c5.metal ²	19000		2375,0		80000	
c5a.large ¹	200	3170	25,00	396,25	800	13300
c5a.xlarge ₁	400	3170	50,00	396,25	1600	13300

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c5a.2xlarge ¹	800	3170	100,00	396,25	3200	13300
c5a.4xlarge ¹	1580	3170	197,50	396,25	6600	13300
c5a.8xlarge ²		3170		396,25		13300
c5a.12xlarge ²		4750		593,75		20 000
c5a.16xlarge ²		6300		787,5		26700
c5a.24xlarge ²		9500		1187,5		40 000
c5ad.large ¹	200	3170	25,00	396,25	800	13300
c5ad.xlarge ¹	400	3170	50,00	396,25	1600	13300
c5ad.2xlarge ¹	800	3170	100,00	396,25	3200	13300
c5ad.4xlarge ¹	1580	3170	197,50	396,25	6600	13300
c5ad.8xlarge ²		3170		396,25		13300

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c5ad.12xlarge ²	4750		593,75		20 000	
c5ad.16xlarge ²	6300		787,5		26700	
c5ad.24xlarge ²	9500		1187,5		40 000	
c5d.large ¹	650	4750	81,25	593,75	4000	20 000
c5d.xlarge ¹	1150	4750	143,75	593,75	6 000	20 000
c5d.2xlarge ¹	2300	4750	287,50	593,75	10 000	20 000
c5d.4xlarge ²	4750		593,75		20 000	
c5d.9xlarge ²	9500		1187,5		40 000	
c5d.12xlarge ²	9500		1187,5		40 000	
c5d.18xlarge ²	19000		2375,0		80000	
c5d.24xlarge ²	19000		2375,0		80000	
c5d.metal ²	19000		2375,0		80000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c5n.large ¹	650	4750	81,25	593,75	4000	20 000
c5n.xlarge ¹	1150	4750	143,75	593,75	6 000	20 000
c5n.2xlarge ¹	2300	4750	287,50	593,75	10 000	20 000
c5n.4xlarge ²		4750		593,75		20 000
c5n.9xlarge ²		9500		1187,5		40 000
c5n.18xlarge ²		19000		2375,0		80000
c5n.metal ²		19000		2375,0		80000
c6a.large ¹	650	10 000	81,25	1250,00	3600	40 000
c6a.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
c6a.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
c6a.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
c6a.8xlarge ²		10 000		1250,0		40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c6a.12xlarge ²	15000			1875,0		60000
c6a.16xlarge ²	20 000			2500,0		80000
c6a.24xlarge ²	30 000			3750,0		120000
c6a.32xlarge ²	40 000			5000,0		160000
c6a.48xlarge ²	40 000			5000,0		240000
c6a.metal ²	40 000			5000,0		240000
c6g.medium ¹	315	4750	39,38	593,75	2500	20 000
c6g.large ¹	630	4750	78,75	593,75	3600	20 000
c6g.xlarge ¹	1188	4750	148,50	593,75	6 000	20 000
c6g.2xlarge ¹	2375	4750	296,88	593,75	12 000	20 000
c6g.4xlarge ²	4750			593,75		20 000
c6g.8xlarge ²	9500			1187,5		40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c6g.12xlarge ²		14250		1781,25		50000
c6g.16xlarge ²		19000		2375,0		80000
c6g.metal ²		19000		2375,0		80000
c6gd.medium ¹	315	4750	39,38	593,75	2500	20 000
c6gd.large ¹	630	4750	78,75	593,75	3600	20 000
c6gd.xlarge ¹	1188	4750	148,50	593,75	6 000	20 000
c6gd.2xlarge ¹	2375	4750	296,88	593,75	12 000	20 000
c6gd.4xlarge ²		4750		593,75		20 000
c6gd.8xlarge ²		9500		1187,5		40 000
c6gd.12xlarge ²		14250		1781,25		50000
c6gd.16xlarge ²		19000		2375,0		80000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c6gd.meta l ²		19000		2375,0		80000
c6gn.medium ¹	760	9500	95,00	1187,50	2500	40 000
c6gn.large ₁	1235	9500	154,38	1187,50	5000	40 000
c6gn.xlarge ¹	2375	9500	296,88	1187,50	10 000	40 000
c6gn.2xlarge ¹	4750	9500	593,75	1187,50	20 000	40 000
c6gn.4xlarge ²		9500		1187,5		40 000
c6gn.8xlarge ²		19000		2375,0		80000
c6gn.12xlarge ²		28500		3562,5		120000
c6gn.16xlarge ²		38000		4750,0		160000
c6i.large ¹	650	10 000	81,25	1250,00	3600	40 000
c6i.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
c6i.2xlarge ₁	2500	10 000	312,50	1250,00	12 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c6i.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
c6i.8xlarge ²		10 000		1250,0		40 000
c6i.12xlarge ²		15000		1875,0		60000
c6i.16xlarge ²		20 000		2500,0		80000
c6i.24xlarge ²		30 000		3750,0		120000
c6i.32xlarge ²		40 000		5000,0		160000
c6i.metal ²		40 000		5000,0		160000
c6id.large ¹	650	10 000	81,25	1250,00	3600	40 000
c6id.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
c6id.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
c6id.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
c6id.8xlarge ²		10 000		1250,0		40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c6id.12xlarge ²	15000			1875,0		60000
c6id.16xlarge ²	20 000			2500,0		80000
c6id.24xlarge ²	30 000			3750,0		120000
c6id.32xlarge ²	40 000			5000,0		160000
c6id.metal ²	40 000			5000,0		160000
c6in.large ¹	1562	25000	195,31	3125,00	6250	100 000
c6in.xlarge ¹	3125	25000	390,62	3125,00	12500	100 000
c6in.2xlarge ¹	6250	25000	781,25	3125,00	25000	100 000
c6in.4xlarge ¹	12500	25000	1562,50	3125,00	50000	100 000
c6in.8xlarge ²	25000			3125,0		100 000
c6in.12xlarge ²	37500			4687,5		150000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c6in.16xlarge ²	50000		6250,0		200 000	
c6in.24xlarge ²	75000		9375,0		300 000	
c6in.32xlarge ²	100 000		12500,0		400 000	
c6in.metal ²	100 000		12500,0		400 000	
c7a.medium ¹	325	10 000	40,62	1250,00	2500	40 000
c7a.large ¹	650	10 000	81,25	1250,00	3600	40 000
c7a.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
c7a.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
c7a.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
c7a.8xlarge ²	10 000		1250,0		40 000	
c7a.12xlarge ²	15000		1875,0		60000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c7a.16xlarge ²	20 000			2500,0		80000
c7a.24xlarge ²	30 000			3750,0		120000
c7a.32xlarge ²	40 000			5000,0		160000
c7a.48xlarge ²	40 000			5000,0		240000
c7a.metal-48xl ²	40 000			5000,0		240000
c7g.medium ¹	315	10 000	39,38	1250,00	2500	40 000
c7g.large ¹	630	10 000	78,75	1250,00	3600	40 000
c7g.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
c7g.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
c7g.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
c7g.8xlarge ²	10 000			1250,0		40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c7g.12xlarge ²	15000			1875,0		60000
c7g.16xlarge ²	20 000			2500,0		80000
c7g.metal ²	20 000			2500,0		80000
c7gd.medium ¹	315	10 000	39,38	1250,00	2500	40 000
c7gd.large ¹	630	10 000	78,75	1250,00	3600	40 000
c7gd.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
c7gd.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
c7gd.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
c7gd.8xlarge ²	10 000			1250,0		40 000
c7gd.12xlarge ²	15000			1875,0		60000
c7gd.16xlarge ²	20 000			2500,0		80000
c7gd.metal 2	20 000			2500,0		80000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c7gn.medium ¹	521	10 000	65,12	1250,00	2083	40 000
c7gn.large ¹	1042	10 000	130,25	1250,00	4167	40 000
c7gn.xlarge ¹	2083	10 000	260,38	1250,00	8333	40 000
c7gn.2xlarge ¹	4167	10 000	520,88	1250,00	16667	40 000
c7gn.4xlarge ¹	8333	10 000	1041,62	1250,00	33333	40 000
c7gn.8xlarge ¹	16667	20 000	2083,38	2500,00	66667	80000
c7gn.12xlarge ¹	25000	30 000	3125,00	3750,00	100 000	120000
c7gn.16xlarge ¹	33333	40 000	4166,62	5000,00	133333	160000
c7gn.metal ¹	33333	40 000	4166,62	5000,00	133333	160000
c7i.large ¹	650	10 000	81,25	1250,00	3600	40 000
c7i.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
c7i.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c7i.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
c7i.8xlarge ²		10 000		1250,0		40 000
c7i.12xlarge ²		15000		1875,0		60000
c7i.16xlarge ²		20 000		2500,0		80000
c7i.24xlarge ²		30 000		3750,0		120000
c7i.48xlarge ²		40 000		5000,0		240000
c7i.metal-24xl ²		30 000		3750,0		120000
c7i.metal-48xl ²		40 000		5000,0		240000
c7i-flex.large ¹	312	10 000	39,06	1250,00	2500	40 000
c7i-flex.xlarge ¹	625	10 000	78,12	1250,00	3600	40 000
c7i-flex.2xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
c7i-flex.4xlarge 1	2500	10 000	312,50	1250,00	12 000	40 000
c7i-flex 8 x large 1	5000	10 000	625,00	1250,00	20 000	40 000

Optimisé pour la mémoire

Important

¹ Ces instances peuvent prendre en charge des performances maximales pendant 30 minutes au moins une fois toutes les 24 heures, délai au-delà duquel elles reviennent à leurs performances de base.

² Ces instances peuvent maintenir leurs performances déclarées indéfiniment. Si votre charge de travail nécessite des performances maximales soutenues pendant plus de 30 minutes, utilisez l'une de ces instances.

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r4.large ²		425		53,125		3000
r4.xlarge ²		850		106,25		6 000
r4.2xlarge ²		1700		212,5		12 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r4.4xlarge ₂	3500		437,5		18750	
r4.8xlarge ₂	7000		875,0		37500	
r4.16xlarge ₂	14000		1750,0		75000	
r5.large ¹	650	4750	81,25	593,75	3600	18750
r5.xlarge ¹	1150	4750	143,75	593,75	6 000	18750
r5.2xlarge ₁	2300	4750	287,50	593,75	12 000	18750
r5.4xlarge ₂	4750		593,75		18750	
r5.8xlarge ₂	6800		850,0		30 000	
r5.12xlarge ₂	9500		1187,5		40 000	
r5.16xlarge ₂	13600		1700,0		60000	
r5.24xlarge ₂	19000		2375,0		80000	
r5.metal ²	19000		2375,0		80000	
r5a.large ¹	650	2880	81,25	360,00	3600	16000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r5a.xlarge ₁	1085	2880	135,62	360,00	6 000	16000
r5a.2xlarge ₁	1580	2880	197,50	360,00	8333	16000
r5a.4xlarge ₂	2880		360,0		16000	
r5a.8xlarge ₂	4750		593,75		20 000	
r5a.12xlarge ₂	6780		847,5		30 000	
r5a.16xlarge ₂	9500		1187,5		40 000	
r5a.24xlarge ₂	13570		1696,25		60000	
r5ad.large ₁	650	2880	81,25	360,00	3600	16000
r5ad.xlarge ₁	1085	2880	135,62	360,00	6 000	16000
r5ad.2xlarge ₁	1580	2880	197,50	360,00	8333	16000
r5ad.4xlarge ₂	2880		360,0		16000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r5ad.8xlarge ²	4750		593,75		20 000	
r5ad.12xlarge ²	6780		847,5		30 000	
r5ad.16xlarge ²	9500		1187,5		40 000	
r5ad.24xlarge ²	13570		1696,25		60000	
r5b.large ¹	1250	10 000	156,25	1250,00	5417	43333
r5b.xlarge ₁	2500	10 000	312,50	1250,00	10833	43333
r5b.2xlarge ₁	5000	10 000	625,00	1250,00	21667	43333
r5b.4xlarge ₂	10 000		1250,0		43333	
r5b.8xlarge ₂	20 000		2500,0		86667	
r5b.12xlarge ²	30 000		3750,0		130000	
r5b.16xlarge ²	40 000		5000,0		173333	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r5b.24xlarge ²		60000		7500,0		260000
r5b.metal ²		60000		7500,0		260000
r5d.large ¹	650	4750	81,25	593,75	3600	18750
r5d.xlarge ₁	1150	4750	143,75	593,75	6 000	18750
r5d.2xlarge ₁	2300	4750	287,50	593,75	12 000	18750
r5d.4xlarge ₂		4750		593,75		18750
r5d.8xlarge ₂		6800		850,0		30 000
r5d.12xlarge ²		9500		1187,5		40 000
r5d.16xlarge ²		13600		1700,0		60000
r5d.24xlarge ²		19000		2375,0		80000
r5d.metal ²		19000		2375,0		80000
r5dn.large ₁	650	4750	81,25	593,75	3600	18750

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r5dn.xlarge ¹	1150	4750	143,75	593,75	6 000	18750
r5dn.2xlarge ¹	2300	4750	287,50	593,75	12 000	18750
r5dn.4xlarge ²		4750		593,75		18750
r5dn.8xlarge ²		6800		850,0		30 000
r5dn.12xlarge ²		9500		1187,5		40 000
r5dn.16xlarge ²		13600		1700,0		60000
r5dn.24xlarge ²		19000		2375,0		80000
r5dn.meta1 ²		19000		2375,0		80000
r5n.large ¹	650	4750	81,25	593,75	3600	18750
r5n.xlarge ¹	1150	4750	143,75	593,75	6 000	18750
r5n.2xlarge ¹	2300	4750	287,50	593,75	12 000	18750

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r5n.4xlarge ²	4750		593,75		18750	
r5n.8xlarge ²	6800		850,0		30 000	
r5n.12xlarge ²	9500		1187,5		40 000	
r5n.16xlarge ²	13600		1700,0		60000	
r5n.24xlarge ²	19000		2375,0		80000	
r5n.metal ²	19000		2375,0		80000	
r6a.large ¹	650	10 000	81,25	1250,00	3600	40 000
r6a.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
r6a.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
r6a.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
r6a.8xlarge ²	10 000		1250,0		40 000	
r6a.12xlarge ²	15000		1875,0		60000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r6a.16xlarge ²	20 000			2500,0		80000
r6a.24xlarge ²	30 000			3750,0		120000
r6a.32xlarge ²	40 000			5000,0		160000
r6a.48xlarge ²	40 000			5000,0		240000
r6a.metal ²	40 000			5000,0		240000
r6g.medium ¹	315	4750	39,38	593,75	2500	20 000
r6g.large ¹	630	4750	78,75	593,75	3600	20 000
r6g.xlarge ¹	1188	4750	148,50	593,75	6 000	20 000
r6g.2xlarge ¹	2375	4750	296,88	593,75	12 000	20 000
r6g.4xlarge ²	4750			593,75		20 000
r6g.8xlarge ²	9500			1187,5		40 000
r6g.12xlarge ²	14250			1781,25		50000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r6g.16xlarge ²	19000		2375,0		80000	
r6g.metal ²	19000		2375,0		80000	
r6gd.medium ¹	315	4750	39,38	593,75	2500	20 000
r6gd.large ¹	630	4750	78,75	593,75	3600	20 000
r6gd.xlarge ¹	1188	4750	148,50	593,75	6 000	20 000
r6gd.2xlarge ¹	2375	4750	296,88	593,75	12 000	20 000
r6gd.4xlarge ²	4750		593,75		20 000	
r6gd.8xlarge ²	9500		1187,5		40 000	
r6gd.12xlarge ²	14250		1781,25		50000	
r6gd.16xlarge ²	19000		2375,0		80000	
r6gd.metal ²	19000		2375,0		80000	
r6i.large ¹	650	10 000	81,25	1250,00	3600	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r6i.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
r6i.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
r6i.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
r6i.8xlarge ²		10 000		1250,0		40 000
r6i.12xlarge ²		15000		1875,0		60000
r6i.16xlarge ²		20 000		2500,0		80000
r6i.24xlarge ²		30 000		3750,0		120000
r6i.32xlarge ²		40 000		5000,0		160000
r6i.metal ²		40 000		5000,0		160000
r6idn.large ¹	1562	25000	195,31	3125,00	6250	100 000
r6idn.xlarge ¹	3125	25000	390,62	3125,00	12500	100 000
r6idn.2xlarge ¹	6250	25000	781,25	3125,00	25000	100 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r6idn.4xlarge ¹	12500	25000	1562,50	3125,00	50000	100 000
r6idn.8xlarge ²	25000	25000	3125,0	3125,0	100 000	100 000
r6idn.12xlarge ²	37500	25000	4687,5	3125,0	150000	100 000
r6idn.16xlarge ²	50000	25000	6250,0	3125,0	200 000	100 000
r6idn.24xlarge ²	75000	25000	9375,0	3125,0	300 000	100 000
r6idn.32xlarge ²	100 000	25000	12500,0	3125,0	400 000	100 000
r6idn.metal ²	100 000	25000	12500,0	3125,0	400 000	100 000
r6in.large ¹	1562	25000	195,31	3125,00	6250	100 000
r6in.xlarge ¹	3125	25000	390,62	3125,00	12500	100 000
r6in.2xlarge ¹	6250	25000	781,25	3125,00	25000	100 000
r6in.4xlarge ¹	12500	25000	1562,50	3125,00	50000	100 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r6in.8xlarge ²	25000			3125,0		100 000
r6in.12xlarge ²	37500			4687,5		150000
r6in.16xlarge ²	50000			6250,0		200 000
r6in.24xlarge ²	75000			9375,0		300 000
r6in.32xlarge ²	100 000			12500,0		400 000
r6in.metal ²	100 000			12500,0		400 000
r6id.large ¹	650	10 000	81,25	1250,00	3600	40 000
r6id.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
r6id.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
r6id.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
r6id.8xlarge ²	10 000			1250,0		40 000
r6id.12xlarge ²	15000			1875,0		60000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r6id.16xlarge ²	20 000			2500,0		80000
r6id.24xlarge ²	30 000			3750,0		120000
r6id.32xlarge ²	40 000			5000,0		160000
r6id.metal ²	40 000			5000,0		160000
r7a.medium ¹	325	10 000	40,62	1250,00	2500	40 000
r7a.large ¹	650	10 000	81,25	1250,00	3600	40 000
r7a.xlarge ₁	1250	10 000	156,25	1250,00	6 000	40 000
r7a.2xlarge ₁	2500	10 000	312,50	1250,00	12 000	40 000
r7a.4xlarge ₁	5000	10 000	625,00	1250,00	20 000	40 000
r7a.8xlarge ₂	10 000			1250,0		40 000
r7a.12xlarge ²	15000			1875,0		60000
r7a.16xlarge ²	20 000			2500,0		80000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r7a.24xlarge ²	30 000			3750,0		120000
r7a.32xlarge ²	40 000			5000,0		160000
r7a.48xlarge ²	40 000			5000,0		240000
r7a.metal-48xl ²	40 000			5000,0		240000
r7g.medium ¹	315	10 000	39,38	1250,00	2500	40 000
r7g.large ¹	630	10 000	78,75	1250,00	3600	40 000
r7g.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
r7g.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
r7g.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
r7g.8xlarge ²	10 000			1250,0		40 000
r7g.12xlarge ²	15000			1875,0		60000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r7g.16xlarge ²	20 000			2500,0		80000
r7g.metal ²	20 000			2500,0		80000
r7gd.medium ¹	315	10 000	39,38	1250,00	2500	40 000
r7gd.large ¹	630	10 000	78,75	1250,00	3600	40 000
r7gd.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
r7gd.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
r7gd.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
r7gd.8xlarge ²	10 000			1250,0		40 000
r7gd.12xlarge ²	15000			1875,0		60000
r7gd.16xlarge ²	20 000			2500,0		80000
r7gd.metal 2	20 000			2500,0		80000
r7i.large ¹	650	10 000	81,25	1250,00	3600	40 000
r7i.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r7i.2xlarge ¹	2500	10 000	312,50	1250,00	12 000	40 000
r7i.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
r7i.8xlarge ²		10 000		1250,0		40 000
r7i.12xlarge ²		15000		1875,0		60000
r7i.16xlarge ²		20 000		2500,0		80000
r7i.24xlarge ²		30 000		3750,0		120000
r7i.48xlarge ²		40 000		5000,0		240000
r7i.metal-24xl ²		30 000		3750,0		120000
r7i.metal-48xl ²		40 000		5000,0		240000
r7iz.large ¹	792	10 000	99,00	1250,00	3600	40 000
r7iz.xlarge ¹	1584	10 000	198,00	1250,00	6667	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
r7iz.2xlarge ¹	3168	10 000	396,00	1250,00	13333	40 000
r7iz.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
r7iz.8xlarge ²		10 000		1250,0		40 000
r7iz.12xlarge ²		19000		2375,0		76000
r7iz.16xlarge ²		20 000		2500,0		80000
r7iz.32xlarge ²		40 000		5000,0		160000
r7iz.meta l-16xl ²		20 000		2500,0		80000
r7iz.meta l-32xl ²		40 000		5000,0		160000
u-3tb1.56xlarge ²		19000		2375,0		80000
u-6tb1.56xlarge ²		38000		4750,0		160000
u-6tb1.112xlarge ²		38000		4750,0		160000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
u-6tb1.metal ²	38000		4750,0		160000	
u-9tb1.112xlarge ²	38000		4750,0		160000	
u-9tb1.metal ²	38000		4750,0		160000	
u-12tb1.112xlarge ²	38000		4750,0		160000	
u-12tb1.metal ²	38000		4750,0		160000	
u-18tb1.112xlarge ²	38000		4750,0		160000	
u-18tb1.metal ²	38000		4750,0		160000	
u-24tb1.112xlarge ²	38000		4750,0		160000	
u-24tb1.metal ²	38000		4750,0		160000	
u7i-12tb.224xlarge2	60000		7500,0		420000	
u7in-16tb.224xlarge2	100 000		12500,0		420000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
u7in-24tb .224xlarge 2	100 000			12500,0		420000
u7in-32tb .224xlarge 2	100 000			12500,0		420000
x1.16xlarge ²	7000			875,0		40 000
x1.32xlarge ²	14000			1750,0		80000
x2gd.medium ¹	315	4750	39,38	593,75	2500	20 000
x2gd.large ¹	630	4750	78,75	593,75	3600	20 000
x2gd.xlarge ¹	1188	4750	148,50	593,75	6 000	20 000
x2gd.2xlarge ¹	2375	4750	296,88	593,75	12 000	20 000
x2gd.4xlarge ²	4750			593,75		20 000
x2gd.8xlarge ²	9500			1187,5		40 000
x2gd.12xlarge ²	14250			1781,25		60000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
x2gd.16xlarge ²	19000			2375,0		80000
x2gd.metal ²	19000			2375,0		80000
x2idn.16xlarge ²	40 000			5000,0		173333
x2idn.24xlarge ²	60000			7500,0		260000
x2idn.32xlarge ²	80000			10000,0		260000
x2idn.metal ²	80000			10000,0		260000
x2iedn.xlarge ¹	2500	20 000	312,50	2500,00	8125	65000
x2iedn.2xlarge ¹	5000	20 000	625,00	2500,00	16250	65000
x2iedn.4xlarge ¹	10 000	20 000	1250,00	2500,00	32500	65000
x2iedn.8xlarge ²	20 000			2500,0		65000
x2iedn.16xlarge ²	40 000			5000,0		130000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
x2iedn.24xlarge ²	60000			7500,0		195 000
x2iedn.32xlarge ²	80000			10000,0		260000
x2iedn.metal ²	80000			10000,0		260000
x2iezn.2xlarge ²	3170			396,25		13333
x2iezn.4xlarge ²	4750			593,75		20 000
x2iezn.6xlarge ²	9500			1187,5		40 000
x2iezn.8xlarge ²	12 000			1500,0		55000
x2iezn.12xlarge ²	19000			2375,0		80000
x2iezn.metal ²	19000			2375,0		80000
x1e.xlarge ²	500			62,5		3700
x1e.2xlarge ²	1 000			125,0		7400

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
x1e.4xlarge ²	1750			218,75		10 000
x1e.8xlarge ²	3500			437,5		20 000
x1e.16xlarge ²	7000			875,0		40 000
x1e.32xlarge ²	14000			1750,0		80000
z1d.large ¹	800	3170	100,00	396,25	3333	13333
z1d.xlarge ¹	1580	3170	197,50	396,25	6667	13333
z1d.2xlarge ²		3170		396,25		13333
z1d.3xlarge ²		4750		593,75		20 000
z1d.6xlarge ²		9500		1187,5		40 000
z1d.12xlarge ²		19000		2375,0		80000
z1d.metal ²		19000		2375,0		80000

Stockage optimisé

⚠ Important

¹ Ces instances peuvent prendre en charge des performances maximales pendant 30 minutes au moins une fois toutes les 24 heures, délai au-delà duquel elles reviennent à leurs performances de base.

² Ces instances peuvent maintenir leurs performances déclarées indéfiniment. Si votre charge de travail nécessite des performances maximales soutenues pendant plus de 30 minutes, utilisez l'une de ces instances.

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
d2.xlarge ²		750		93,75		6 000
d2.2xlarge ²		1 000		125,0		8000
d2.4xlarge ²		2000		250,0		16000
d2.8xlarge ²		4000		500,0		32000
d3.xlarge ¹	850	2800	106,25	350,00	5000	15000
d3.2xlarge ¹	1700	2800	212,50	350,00	10 000	15000
d3.4xlarge ²		2800		350,0		15000
d3.8xlarge ²		5000		625,0		30 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
d3en.xlarge ¹	850	2800	106,25	350,00	5000	15000
d3en.2xlarge ¹	1700	2800	212,50	350,00	10 000	15000
d3en.4xlarge ²		2800		350,0		15000
d3en.6xlarge ²		4000		500,0		25000
d3en.8xlarge ²		5000		625,0		30 000
d3en.12xlarge ²		7000		875,0		40 000
h1.2xlarge ²		1750		218,75		12 000
h1.4xlarge ²		3500		437,5		20 000
h1.8xlarge ²		7000		875,0		40 000
h1.16xlarge ²		14000		1750,0		80000
i3.large ²		425		53,125		3000
i3.xlarge ²		850		106,25		6 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
i3.2xlarge ²		1700		212,5		12 000
i3.4xlarge ²		3500		437,5		16000
i3.8xlarge ²		7000		875,0		32500
i3.16xlarge ²		14000		1750,0		65000
i3.metal ²		19000		2375,0		80000
i3en.large ¹	576	4750	72,10	593,75	3000	20 000
i3en.xlarge ¹	1153	4750	144,20	593,75	6 000	20 000
i3en.2xlarge ¹	2307	4750	288,39	593,75	12 000	20 000
i3en.3xlarge ¹	3800	4750	475,00	593,75	15000	20 000
i3en.6xlarge ²		4750		593,75		20 000
i3en.12xlarge ²		9500		1187,5		40 000
i3en.24xlarge ²		19000		2375,0		80000
i3en.metal ²		19000		2375,0		80000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
i4g.large ¹	625	10 000	78,12	1250,00	2500	40 000
i4g.xlarge ¹	1250	10 000	156,25	1250,00	5000	40 000
i4g.2xlarge ¹	2500	10 000	312,50	1250,00	10 000	40 000
i4g.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
i4g.8xlarge ²		10 000		1250,0		40 000
i4g.16xlarge ²		20 000		2500,0		80000
i4i.large ¹	625	10 000	78,12	1250,00	2500	40 000
i4i.xlarge ¹	1250	10 000	156,25	1250,00	5000	40 000
i4i.2xlarge ¹	2500	10 000	312,50	1250,00	10 000	40 000
i4i.4xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
i4i.8xlarge ²		10 000		1250,0		40 000
i4i.12xlarge ²		15000		1875,0		60000
i4i.16xlarge ²		20 000		2500,0		80000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
i4i.24xlarge ²	30 000			3750,0		120000
i4i.32xlarge ²	40 000			5000,0		160000
i4i.metal ²	40 000			5000,0		160000
im4gn.large ¹	1250	10 000	156,25	1250,00	5000	40 000
im4gn.xlarge ¹	2500	10 000	312,50	1250,00	10 000	40 000
im4gn.2xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
im4gn.4xlarge ²	10 000			1250,0		40 000
im4gn.8xlarge ²	20 000			2500,0		80000
im4gn.16xlarge ²	40 000			5000,0		160000
is4gen.medium ¹	625	10 000	78,12	1250,00	2500	40 000
is4gen.large ¹	1250	10 000	156,25	1250,00	5000	40 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
is4gen.xlarge ¹	2500	10 000	312,50	1250,00	10 000	40 000
is4gen.2xlarge ¹	5000	10 000	625,00	1250,00	20 000	40 000
is4gen.4xlarge ²		10 000		1250,0		40 000
is4gen.8xlarge ²		20 000		2500,0		80000

Calcul accéléré

Important

¹ Ces instances peuvent prendre en charge des performances maximales pendant 30 minutes au moins une fois toutes les 24 heures, délai au-delà duquel elles reviennent à leurs performances de base.

² Ces instances peuvent maintenir leurs performances déclarées indéfiniment. Si votre charge de travail nécessite des performances maximales soutenues pendant plus de 30 minutes, utilisez l'une de ces instances.

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
dl1.24xlarge ²	19000		2375,0		80000	
dl2q.24xlarge ²	19000		2375,0		80000	
f1.2xlarge ²	1700		212,5		12 000	
f1.4xlarge ²	3500		437,5		44000	
f1.16xlarge ²	14000		1750,0		75000	
g3.4xlarge ²	3500		437,5		20 000	
g3.8xlarge ²	7000		875,0		40 000	
g3.16xlarge ²	14000		1750,0		80000	
g4ad.xlarge ¹	400	3170	50,00	396,25	1700	13333
g4ad.2xlarge ¹	800	3170	100,00	396,25	3400	13333
g4ad.4xlarge ¹	1580	3170	197,50	396,25	6700	13333
g4ad.8xlarge ²		3170		396,25		13333

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
g4ad.16xlarge ²		6300		787,5		26667
g4dn.xlarge ¹	950	3500	118,75	437,50	3000	20 000
g4dn.2xlarge ¹	1150	3500	143,75	437,50	6 000	20 000
g4dn.4xlarge ²		4750		593,75		20 000
g4dn.8xlarge ²		9500		1187,5		40 000
g4dn.12xlarge ²		9500		1187,5		40 000
g4dn.16xlarge ²		9500		1187,5		40 000
g4dn.meta1 ²		19000		2375,0		80000
g5.xlarge ¹	700	3500	87,50	437,50	3000	15000
g5.2xlarge ¹	850	3500	106,25	437,50	3500	15000
g5.4xlarge ²		4750		593,75		20 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
g5.8xlarge ²	16000			2000,0		65000
g5.12xlarge ²	16000			2000,0		65000
g5.16xlarge ²	16000			2000,0		65000
g5.24xlarge ²	19000			2375,0		80000
g5.48xlarge ²	19000			2375,0		80000
g5g.xlarge ¹	1188	4750	148,50	593,75	6 000	20 000
g5g.2xlarge ¹	2375	4750	296,88	593,75	12 000	20 000
g5g.4xlarge ²	4750			593,75		20 000
g5g.8xlarge ²	9500			1187,5		40 000
g5g.16xlarge ²	19000			2375,0		80000
g5g.metal ²	19000			2375,0		80000
g6.xlarge ¹	1 000	5000	125,00	625,00	4000	20 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
g6,2 x large 1	2000	5000	250,00	625,00	8000	20 000
g6,4xlarge 2	8000		1000,0		32000	
g 6,8 x large 2	16000		2000,0		64000	
g 6,12 x large 2	20 000		2500,0		80000	
g 6,16 x large 2	20 000		2500,0		80000	
g 6,24 x large 2	30 000		3750,0		120000	
g 6,48 x large 2	60000		7500,0		240000	
gr6,4xlarge 2	8000		1000,0		32000	
gr6,8xlarge 2	16000		2000,0		64000	
inf1.xlarge 1	1190	4750	148.75	593,75	4000	20 000
inf1.2xlarge 1	1190	4750	148.75	593,75	6 000	20 000
inf1.6xlarge 2	4750		593,75		20 000	
inf1.24xlarge 2	19000		2375,0		80000	

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
inf2.xlarge ¹	1250	10 000	156,25	1250,00	6 000	40 000
inf2.8xlarge ²		10 000		1250,0		40 000
inf2.24xlarge ²		30 000		3750,0		120000
inf2.48xlarge ²		60000		7500,0		240000
p2.xlarge ²		750		93,75		6 000
p2.8xlarge ²		5000		625,0		32500
p2.16xlarge ²		10 000		1250,0		65000
p3.2xlarge ²		1750		218,75		10 000
p3.8xlarge ²		7000		875,0		40 000
p3.16xlarge ²		14000		1750,0		80000
p3dn.24xlarge ²		19000		2375,0		80000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
p4d.24xlarge ²	19000		2375,0		80000	
p4de.24xlarge ²	19000		2375,0		80000	
p5.48xlarge ²	80000		10000,0		260000	
trn1.2xlarge ¹	5000	20 000	625,00	2500,00	16250	65000
trn1.32xlarge ²	80000		10000,0		260000	
trn1n.32xlarge ²	80000		10000,0		260000	
vt1.3xlarge ¹	2375	4750	296,88	593,75	10 000	20 000
vt1.6xlarge ²	4750		593,75		20 000	
vt1.24xlarge ²	19000		2375,0		80000	

Calcul haute performance

⚠ Important

¹ Ces instances peuvent prendre en charge des performances maximales pendant 30 minutes au moins une fois toutes les 24 heures, délai au-delà duquel elles reviennent à leurs performances de base.

² Ces instances peuvent maintenir leurs performances déclarées indéfiniment. Si votre charge de travail nécessite des performances maximales soutenues pendant plus de 30 minutes, utilisez l'une de ces instances.

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
hpc6a.48xlarge ¹	87	2085	10,88	260,62	500	11 000
hpc6id.32xlarge ¹	87	2085	10,88	260,62	500	11 000
hpc7a.12xlarge ¹	87	2085	10,88	260,62	500	11 000
hpc7a.24xlarge ¹	87	2085	10,88	260,62	500	11 000
hpc7a.48xlarge ¹	87	2085	10,88	260,62	500	11 000
hpc7a.96xlarge ¹	87	2085	10,88	260,62	500	11 000
hpc7g.4xlarge ¹	87	2085	10,88	260,62	500	11 000

Taille d'instance	Bande passante de référence (Mbit/s)	Bande passante maximum (Mbit/s)	Débit de référence (Mbit/s, I/O de 128 Kio)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS de référence (I/O de 16 Kio)	IOPS maximum (I/O de 16 Kio)
hpc7g.8xlarge ¹	87	2085	10,88	260,62	500	11 000
hpc7g.16xlarge ¹	87	2085	10,88	260,62	500	11 000

Optimisation EBS prise en charge

Le tableau suivant présente les types d'instance qui prennent en charge l'optimisation EBS par défaut, mais pour lesquels cette optimisation n'est pas activée par défaut. Vous pouvez activer l'optimisation EBS lorsque vous lancez ces instances ou lorsqu'elles sont en cours d'exécution. L'optimisation EBS doit être activée sur les instances afin d'atteindre le niveau de performance décrit. Lorsque vous activez l'optimisation EBS pour une instance qui n'est pas optimisée EBS par défaut, vous payez un droit horaire supplémentaire peu élevé pour la capacité dédiée. Pour plus d'informations sur la tarification, consultez Instances optimisées EBS sur la [page Tarification Amazon EC2, Tarification à la demande](#).

Note

Vous pouvez également consulter ces informations par programme à l'aide du AWS CLI. Pour plus d'informations, consultez [Afficher les types d'instances qui prennent en charge l'optimisation EBS](#).

Taille d'instance	Bande passante maximum (Mbit/s)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS maximum (I/O de 16 Kio)
c1.xlarge	1 000	125,0	8000
c3.xlarge	500	62,5	4000

Taille d'instance	Bande passante maximum (Mbit/s)	Débit maximal (Mbit/s, I/O de 128 Kio)	IOPS maximum (I/O de 16 Kio)
c3.2xlarge	1 000	125,0	8000
c3.4xlarge	2000	250,0	16000
i2.xlarge	500	62,5	4000
i2.2xlarge	1 000	125,0	8000
i2.4xlarge	2000	250,0	16000
m1.large	500	62,5	4000
m1.xlarge	1 000	125,0	8000
m2.2xlarge	500	62,5	4000
m2.4xlarge	1 000	125,0	8000
m3.xlarge	500	62,5	4000
m3.2xlarge	1 000	125,0	8000
r3.xlarge	500	62,5	4000
r3.2xlarge	1 000	125,0	8000
r3.4xlarge	2000	250,0	16000

Les instances `i2.8xlarge`, `c3.8xlarge` et `r3.8xlarge` ne disposent pas de bande passante EBS dédiée et n'offrent donc pas d'optimisation EBS. Sur ces instances, le trafic réseau et le trafic Amazon EBS partagent la même interface réseau 10 gigabits.

Obtenir les performances maximales

Vous pouvez utiliser les métriques `EBSIOBalance%` et `EBSByteBalance%` pour déterminer si vos instances sont dimensionnées correctement. Vous pouvez consulter ces mesures dans la CloudWatch console et définir une alarme qui sera déclenchée en fonction d'un seuil que vous

spécifiez. Ces métriques sont exprimées sous forme de pourcentage. Les instances avec un pourcentage d'équilibre constamment faible sont candidates pour une augmentation de leur taille. Les instances pour lesquelles le pourcentage d'équilibre ne descend jamais sous 100 % sont candidates pour une diminution de leur taille. Pour plus d'informations, consultez [Surveillez vos instances à l'aide de CloudWatch](#).

Les instances à mémoire élevée sont conçues pour exécuter d'importantes bases de données en mémoire, notamment des déploiements en production de la base de données en mémoire SAP HANA, dans le Cloud. Pour optimiser les performances EBS, utilisez des instances à mémoire élevée avec un nombre pair de volumes `io1` ou `io2` avec des performances provisionnées identiques. Par exemple, pour les charges de travail lourdes d'I/O par seconde, utilisez quatre volumes `io1` ou `io2` avec 40 000 I/O par seconde provisionnées pour obtenir le maximum de 160 000 I/O par seconde d'instance. De même, pour les charges de travail lourdes à débit, utilisez six volumes `io1` ou `io2` avec 48 000 I/O par seconde provisionnées pour obtenir le débit maximal de 4 750 Mo/s. Pour plus de recommandations, consultez [Configuration du stockage pour SAP HANA](#).

Considérations

- Les instances `G4dn`, `i3en`, `M5a`, `M5ad`, `R5a`, `R5ad`, `T3`, `T3a` et `Z1d` lancées après le 26 février 2020 fournissent les performances maximales indiquées dans le tableau ci-dessus. Pour obtenir les performances maximales d'une instance lancée avant le 26 février 2020, arrêtez-la et démarrez-la.
- Les instances `C5`, `C5d`, `C5n`, `M5`, `M5d`, `M5n`, `M5dn`, `R5`, `R5d`, `R5n`, `R5dn` et `P3dn` lancées après le 3 décembre 2019 fournissent les performances maximales indiquées dans le tableau ci-dessus. Pour obtenir les performances maximales d'une instance lancée avant le 3 décembre 2019, arrêtez-la et démarrez-la.
- Les instances `u-6tb1.metal`, `u-9tb1.metal` et `u-12tb1.metal` lancées après le 12 mars 2020 fournissent les performances indiquées dans le tableau ci-dessus. Les instances de ce type lancées avant le 12 mars 2020 sont susceptibles de fournir des performances inférieures. Pour obtenir les performances maximales d'une instance lancée avant le 12 mars 2020, contactez votre équipe de compte pour mettre à niveau l'instance sans frais supplémentaires.

Afficher les types d'instances qui prennent en charge l'optimisation EBS

Vous pouvez utiliser le AWS CLI pour afficher les types d'instances de la région actuelle qui prennent en charge l'optimisation EBS.

Pour afficher les types d'instance qui prennent en charge l'optimisation EBS et pour lesquels cette optimisation est activée par défaut

Utilisez la commande [suivante de 'describe-instance-types'](#). Si vous exécutez cette commande depuis une invite de commandes Windows, remplacez les caractères de suite \ line par le caractère ^.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIOPS,"MaxThroughput(MB/s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=default --output=table
```

Exemple de sortie pour eu-west-1 :

```
-----
|                               DescribeInstanceTypes                               |
+-----+-----+-----+-----+
| InstanceType | MaxBandwidth(Mb/s) | MaxIOPS | MaxThroughput(MB/s) |
+-----+-----+-----+-----+
| m5dn.8xlarge | 6800                | 30000  | 850.0               |
| m6gd.xlarge  | 4750                | 20000  | 593.75              |
| c4.4xlarge   | 2000                | 16000  | 250.0               |
| r4.16xlarge  | 14000               | 75000  | 1750.0              |
| m5ad.large   | 2880                | 16000  | 360.0               |
| ...          |                     |         |                     |
-----
```

Pour afficher les types d'instance qui prennent en charge l'optimisation EBS par défaut, mais pour lesquels cette optimisation n'est pas activée par défaut

Utilisez la commande [suivante de 'describe-instance-types'](#).

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIOPS,"MaxThroughput(MB/s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=supported --output=table
```

Exemple de sortie pour eu-west-1 :

```
-----
```

DescribeInstanceTypes			
InstanceType	MaxBandwidth(Mb/s)	MaxIOPS	MaxThroughput(MB/s)
i2.2xlarge	1000	8000	125.0
m2.4xlarge	1000	8000	125.0
m2.2xlarge	500	4000	62.5
c1.xlarge	1000	8000	125.0
i2.xlarge	500	4000	62.5
m3.xlarge	500	4000	62.5
m1.xlarge	1000	8000	125.0
r3.4xlarge	2000	16000	250.0
r3.2xlarge	1000	8000	125.0
c3.xlarge	500	4000	62.5
m3.2xlarge	1000	8000	125.0
r3.xlarge	500	4000	62.5
i2.4xlarge	2000	16000	250.0
c3.4xlarge	2000	16000	250.0
c3.2xlarge	1000	8000	125.0
m1.large	500	4000	62.5

Activer l'optimisation EBS au lancement

Vous pouvez activer cette optimisation pour une instance en paramétrant son attribut pour l'optimisation EBS.

Pour activer l'optimisation Amazon EBS lors du lancement d'une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Launch Instances.
3. Dans Step 1: Choose an Amazon Machine Image (AMI), sélectionnez une AMI.
4. Dans Step 2: Choose an Instance Type, sélectionnez un type d'instance affiché comme prenant en charge l'optimisation Amazon EBS.
5. Dans Step 3: Configure Instance Details, renseignez les champs nécessaires et choisissez Launch as EBS-optimized instance. Si le type d'instance que vous avez sélectionné dans l'étape précédente ne prend pas en charge l'optimisation Amazon EBS, cette option n'est pas présente. Si le type d'instance que vous avez sélectionné est optimisé pour Amazon EBS par défaut, cette option est activée et vous ne pouvez pas la désactiver.
6. Suivez les instructions pour terminer l'Assistant et lancer votre instance.

Pour activer l'optimisation EBS lors du lancement d'une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes avec l'option correspondante. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [run-instances](#) avec `--ebs-optimized` (AWS CLI)
- [New-EC2Instance](#) avec `-EbsOptimized` (AWS Tools for Windows PowerShell)

Activer l'optimisation EBS pour une instance existante

Vous pouvez activer ou désactiver l'optimisation pour une instance en cours d'exécution en modifiant son attribut d'instance optimisée pour Amazon EBS. Si l'instance est en cours d'exécution, vous devez d'abord l'arrêter.

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

Pour activer l'optimisation EBS d'une instance existante à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances, puis choisissez l'instance.
3. Sélectionnez l'instance et choisissez Actions, État de l'instance, Arrêter l'instance. L'arrêt de l'instance peut prendre quelques minutes.
4. Tandis que l'instance est toujours sélectionnée, choisissez Actions, Paramètres de l'instance, puis Changer le type d'instance.
5. Pour Modifier le type d'instance, effectuez l'une des opérations suivantes :
 - Si le type de votre instance est optimisé pour Amazon EBS par défaut, l'option Optimisé pour EBS est activé et vous ne pouvez pas la modifier. Vous pouvez choisir Annuler, car l'optimisation Amazon EBS est déjà activée pour l'instance.
 - Si le type de votre instance prend en charge l'optimisation Amazon EBS, choisissez Optimisé pour EBS, puis choisissez Appliquer.

- Si le type de votre instance ne prend pas en charge l'optimisation Amazon EBS, vous ne pouvez pas choisir l'option Optimisé pour EBS. Vous pouvez sélectionner un type d'instance à partir de Type d'instance qui prend en charge l'optimisation Amazon EBS, puis choisir Optimisé pour EBS et Appliquer.
6. Choisissez État de l'instance, Démarrer l'instance.

Pour activer l'optimisation EBS d'une instance en cours d'exécution à l'aide de la ligne de commande

1. Si l'instance est en cours d'exécution, utilisez l'une des commandes suivantes pour l'arrêter :
 - [stop-instances](#) (AWS CLI)
 - [Stop-EC2Instance](#) (AWS Tools for Windows PowerShell)
2. Pour activer l'optimisation EBS, utilisez l'une des commandes suivantes avec l'option correspondante :
 - [modify-instance-attribute](#) avec `--ebs-optimized` (AWS CLI)
 - [Edit-EC2InstanceAttribute](#) avec `-EbsOptimized` (AWS Tools for Windows PowerShell)

Options d'achat d'instance

Amazon EC2 propose les options d'achat suivantes pour vous permettre d'optimiser vos coûts en fonction de vos besoins :

- [Instances à la demande](#) – Payez à la seconde pour les instances que vous lancez.
- [Savings Plans](#) (Plans d'économies) – Réduisez vos coûts Amazon EC2 en vous engageant pour une utilisation continue, en USD par heure, pour une durée de 1 à 3 ans.
- [Instances réservées](#) – Réduisez vos coûts Amazon EC2 en vous engageant pour une configuration d'instance continue, incluant le type et la région, pour une durée de 1 à 3 ans.
- [Instances Spot](#) – Demandez des instances EC2 inutilisées, ce qui peut réduire vos coûts Amazon EC2 de façon considérable.
- [Hôtes dédiés](#) – Paiement d'un hôte physique qui est entièrement dédié à l'exécution de vos instances et utilisation du modèle BYOL (Bring-Your-Own-License) pour vos licences logicielles par socket, par cœur ou par ordinateur virtuel afin de réduire les coûts.
- [Instances dédiées](#) – Payez à l'heure, pour les instances qui s'exécutent sur un matériel à client unique.

- [Réservations de capacité](#) : réservez de la capacité pour vos instances EC2 dans une zone de disponibilité spécifique.

Si vous ne pouvez pas vous engager sur une configuration d'instance spécifique, mais que vous pouvez vous engager sur un montant d'utilisation, achetez des Savings Plans pour réduire les coûts de vos instances à la demande. Si vous avez besoin d'une réservation de capacité, achetez des instances réservées ou des réservations de capacité pour une zone de disponibilité spécifique. Les blocs de capacité peuvent être utilisés pour réserver un cluster d'instances GPU. Les instances Spot constituent un choix économique si vous êtes flexible quant au moment où vos applications s'exécutent et à la possibilité de les interrompre. Les hôtes dédiés ou les instances dédiées peuvent vous aider à satisfaire vos exigences en matière de conformité et à réduire les coûts en utilisant vos licences logicielles existantes liées au serveur. Pour plus d'informations, consultez [Tarification Amazon EC2](#).

Pour en savoir plus sur les Savings Plans, consultez le [Guide de l'utilisateur des Savings Plans](#).

Sommaire

- [Déterminer le cycle de vie de l'instance](#)
- [On-Demand instances](#)
- [Reserved instances](#)
- [Spot instances](#)
- [Hôtes dédiés](#)
- [Dedicated instances](#)
- [Réserve de capacité](#)

Déterminer le cycle de vie de l'instance

Le cycle de vie d'une instance démarre au lancement de l'instance et prend fin à sa résiliation. L'option d'achat que vous choisissez affecte le cycle de vie de l'instance. Par exemple, une instance à la demande s'exécute lorsque vous la lancez et prend fin lorsque vous la résiliez. Une instance Spot s'exécute aussi longtemps que la capacité est disponible et que le prix maximum de votre offre est supérieur au prix Spot.

Utilisez l'une des méthodes suivantes pour déterminer le cycle de vie d'une instance.

Pour déterminer le cycle de vie d'une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Sous l'onglet Détails, sous Détails de l'instance, recherchez Cycle de vie. Si la valeur est `spot`, l'instance est une instance Spot. Si la valeur est `normal`, l'instance est une instance à la demande ou une Instance réservée.
5. Sous l'onglet Détails, sous Hôte et groupe de placement, recherchez Locataire. Si la valeur est `host`, l'instance s'exécute sur un Hôte dédié. Si la valeur est `dedicated`, l'instance est une Instance dédiée.

Pour déterminer le cycle de vie de l'instance à l'aide du AWS CLI

Utilisez la commande [describe-instances](#) suivante :

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0
```

Si l'instance s'exécute sur un Hôte dédié, la sortie contient les informations suivantes :

```
"Tenancy": "host"
```

Si l'instance est une Instance dédiée, la sortie contient les informations suivantes :

```
"Tenancy": "dedicated"
```

Si l'instance est une instance Spot, la sortie contient les informations suivantes :

```
"InstanceLifecycle": "spot"
```

Sinon, la sortie ne contient pas `InstanceLifecycle`.

On-Demand instances

Avec les instances à la demande, vous payez la capacité de calcul à la seconde, sans engagement à long terme. Vous bénéficiez d'un contrôle complet sur le cycle de vie de l'instance : vous décidez quand la lancer, l'arrêter, la mettre en veille prolongée, la démarrer, la redémarrer ou la résilier.

Aucun engagement à long terme n'est requis lorsque vous achetez des instances à la demande. Vous payez uniquement pour les secondes pendant lesquelles vos Instances à la demande sont à l'état `running`, avec un minimum de 60 secondes. Le prix par seconde pour une instance à la demande en cours d'exécution est fixe. Il figure sur la page [Amazon EC2 Pricing, On-Demand Pricing](#) (Tarification Amazon EC2, Tarification à la demande), page (Tarification Amazon EC2).

Nous vous recommandons d'utiliser des instances à la demande pour les applications avec des charges de travail irrégulières à court terme qui ne peuvent pas être interrompues.

Pour réaliser des économies importantes par rapport aux instances à la demande, utilisez [AWS Savings Plans](#), [Spot instances](#) ou [Reserved instances](#).

Table des matières

- [Quotas des instances à la demande](#)
 - [Surveiller les quotas et l'utilisation des instances à la demande](#)
 - [Demander une augmentation de quota](#)
- [Rechercher les prix des instances à la demande](#)

Quotas des instances à la demande

Il existe des quotas pour le nombre d'instances à la demande en cours d'exécution Compte AWS par région. Les quotas des instances à la demande sont gérés en termes de nombre d'unités centrales virtuelles (vCPU) que vos instances à la demande en cours d'exécution utilisent, quel que soit le type d'instance. Chaque type de quota spécifie le nombre maximum de vCPU pour une ou plusieurs familles d'instances.

Votre compte inclut les quotas suivants pour les instances à la demande. Les quotas s'appliquent uniquement aux instances en cours d'exécution. Si votre instance est en attente, à l'arrêt, arrêtée ou mise en veille prolongée, elle n'est pas prise en compte dans vos quotas.

Nom	Par défaut	Ajustable
Les instances DL à la demande en cours d'exécution	0	Oui
Instances F à la demande en cours d'exécution	0	Oui
Les instances G et VT à la demande en cours d'exécution	0	Oui

Nom	Par défaut	Ajustable
Les instances HPC à la demande en cours d'exécution	0	Oui
Toutes les instances mémoire élevée à la demande en cours d'exécution	0	Oui
Instances Inf à la demande en cours d'exécution	0	Oui
Instances P à la demande en cours d'exécution	0	Oui
Les instances standard à la demande (A, C, D, H, I, M, R, T, Z) en cours d'exécution	5	Oui
Les instances Trn à la demande en cours d'exécution	0	Oui
Instances X à la demande en cours d'exécution	0	Oui

Pour plus d'informations sur les différentes familles, générations et tailles d'instances, consultez le guide des [types d'instances Amazon EC2](#).

Vous pouvez lancer toute combinaison de types d'instance qui répond à l'évolution de vos besoins en termes d'applications, tant que le nombre de vCPU ne dépasse pas le quota de votre compte. Par exemple, avec un quota d'instances standard de 256 vCPU, vous pouvez lancer 32 instances `m5.2xlarge` (32 x 8 vCPU) ou 16 instances `c5.4xlarge` (16 x 16 vCPU). Pour plus d'informations, consultez [Limites d'instance à la demande EC2](#).

Tâches

- [Surveiller les quotas et l'utilisation des instances à la demande](#)
- [Demander une augmentation de quota](#)

Surveiller les quotas et l'utilisation des instances à la demande

Vous pouvez afficher et gérer les quotas de vos instances à la demande pour chaque région en utilisant les méthodes suivantes.

Pour afficher vos quotas actuels à l'aide de la console Service Quotas

1. Ouvrez la console Service Quotas à l'adresse <https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/>.
2. Dans la barre de navigation, sélectionnez une région.
3. Dans le champ de filtre, saisissez **On-Demand**.
4. La colonne Valeur du quota appliqué affiche le nombre maximum de vCPU pour chaque type de quota des instances à la demande de votre compte.

Pour consulter vos quotas actuels à l'aide de la AWS Trusted Advisor console

Ouvrez la [page des limites de service](#) dans la AWS Trusted Advisor console.

Pour configurer les CloudWatch alarmes

Grâce à l'intégration CloudWatch des métriques Amazon, vous pouvez surveiller votre utilisation d'EC2 par rapport à vos quotas. Vous pouvez également configurer des alarmes pour vous avertir lorsque vous approchez des quotas. Pour plus d'informations, consultez les sections [Service Quotas et Amazon CloudWatch alarmes](#) dans le Guide de l'utilisateur de Service Quotas.

Demander une augmentation de quota

Même si Amazon EC2 augmente automatiquement les quotas de vos instances à la demande en fonction de votre utilisation, vous pouvez demander une augmentation de quota si nécessaire. Par exemple, si vous avez l'intention de lancer plus d'instances que celles autorisées par votre quota actuel, vous pouvez demander une augmentation de quota à l'aide de la console Service Quotas, comme décrit dans [Quotas de service Amazon EC2](#).

Rechercher les prix des instances à la demande

Vous pouvez utiliser l'API du service de liste de prix ou l'API de liste de prix AWS pour demander les prix des instances à la demande. Pour plus d'informations, consultez la section [Utilisation de l'API AWS Price List](#) dans le guide de AWS Billing l'utilisateur.

Reserved instances

Important

Nous recommandons les Savings Plans plutôt que les instances réservées. Les plans d'épargne constituent le moyen le plus simple et le plus flexible d'économiser de l'argent sur

vos coûts de AWS calcul et de proposer des prix plus bas (jusqu'à 72 % de réduction sur les prix à la demande), tout comme les instances réservées. Cependant, les Savings Plans sont différents des instances réservées. Avec les instances réservées, vous vous engagez à utiliser une configuration d'instance spécifique, tandis qu'avec Savings Plans, vous avez la possibilité d'utiliser les configurations d'instance qui répondent le mieux à vos besoins. Pour utiliser Savings Plans, vous vous engagez à utiliser un montant d'utilisation constant, mesuré en dollars américains par heure. Pour plus d'informations, consultez le [Guide de l'utilisateur des AWS Savings Plans](#).

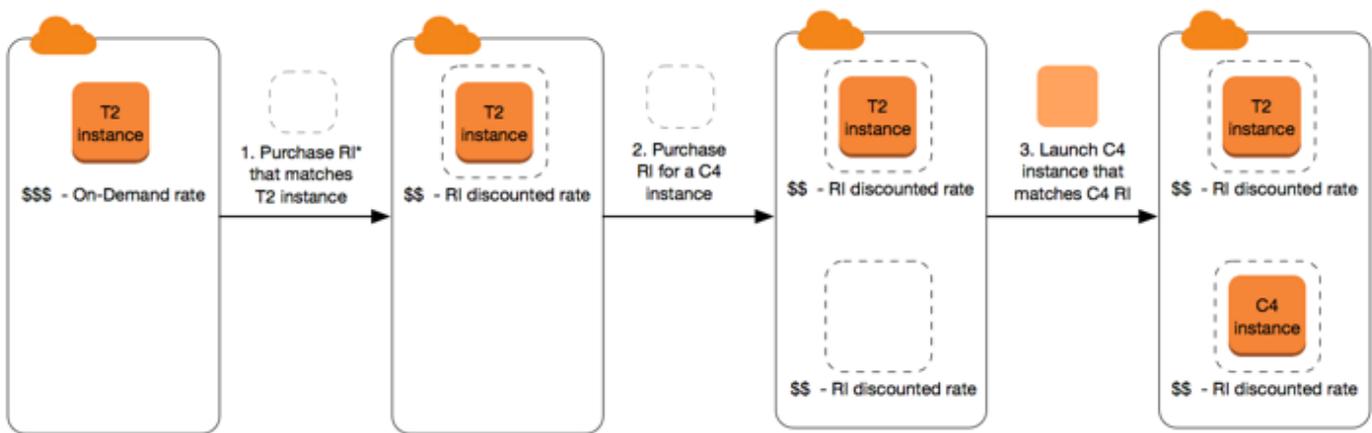
Les instances réservées vous permettent de réaliser d'importantes économies sur vos coûts Amazon EC2 en comparaison de la tarification des instances à la demande. Les instances réservées ne sont pas des instances physiques, mais correspondent à une remise de facturation appliquée à l'utilisation d'instances à la demande dans votre compte. Ces instances à la demande doivent correspondre à certains attributs, comme le type et la région de l'instance, afin d'entraîner une remise de facturation.

Rubriques instances réservées

- [Présentation de Instance réservée](#)
- [Variables clés déterminant la tarification d'une Instance réservée](#)
- [instances réservées régionales et zonales \(portée\)](#)
- [Types d'instances réservées \(classes d'offres\)](#)
- [Application des instances réservées](#)
- [Utiliser votre instances réservées](#)
- [Principes de facturation](#)
- [Acheter des instances réservées](#)
- [Vendre sur la marketplace des instances réservées](#)
- [Modifier instances réservées](#)
- [Échanger des instances réservées convertibles](#)
- [Quotas d'instances réservées](#)

Présentation de Instance réservée

Le schéma suivant montre une vue d'ensemble élémentaire de l'achat et de l'utilisation des instances réservées.



*RI = Reserved Instance

Dans ce scénario, vous disposez dans votre compte d'une instance à la demande (T2) en cours d'exécution, qui vous est facturée au tarif à la demande. Vous achetez une Instance réservée qui correspond aux attributs de votre instance en cours d'exécution et l'avantage de facturation est immédiatement appliqué. Ensuite, vous achetez une Instance réservée pour une instance C4. Aucune instance en cours d'exécution dans votre compte ne correspond aux attributs de cette Instance réservée. Dans la dernière étape, vous lancez une instance qui correspond aux attributs de l'Instance réservée C4 et l'avantage de facturation est immédiatement appliqué.

Variables clés déterminant la tarification d'une Instance réservée

La tarification de Instance réservée est déterminée par les variables clés suivantes.

Attributs d'instance

Une instance réservée dispose de quatre attributs d'instance qui déterminent son prix.

- **Type d'instance :** par exemple, `m4.large`. Il est composé de la famille de l'instance (par exemple, `m4`) et de la taille de l'instance (par exemple, `large`).
- **Région :** Région dans laquelle l'Instance réservée a été achetée.
- **Location :** si votre instance est exécutée sur un matériel partagé (par défaut) ou à client unique (dédié). Pour plus d'informations, consultez [Dedicated instances](#).
- **Plateforme :** le système d'exploitation ; par exemple, Windows ou Linux/Unix. Pour plus d'informations, consultez [Sélection d'une plateforme](#).

Engagement de durée

Vous pouvez acheter une Instance réservée pour un engagement d'un ou de trois ans, avec une remise plus importante pour l'engagement de trois ans.

- Un an : un an correspond à 31536000 secondes (365 jours).
- Trois ans : trois ans correspondent à 94608000 secondes (1095 jours).

Les instances réservées ne sont pas renouvelées automatiquement. Lorsqu'elles expirent, vous pouvez continuer à utiliser l'instance EC2 sans interruption, mais elle est facturée aux tarifs à la demande. Dans l'exemple ci-dessus, lorsque les instances réservées qui couvrent les instances T2 et C4 expirent, les tarifs à la demande vous sont à nouveaux appliqués jusqu'à ce que vous mettiez les instances hors service ou que vous achetiez de nouvelles instances réservées qui correspondent aux attributs de l'instance.

Important

Une fois que vous avez acheté une Instance réservée, vous ne pouvez pas annuler votre achat. Toutefois, vous pourrez probablement [modifier](#), [échanger](#) ou [vendre](#) votre Instance réservée si vos besoins évoluent.

Options de paiement

Les options de paiement suivantes sont disponibles pour les instances réservées :

- Tous les frais initiaux : le paiement est effectué en totalité au début de la période, sans aucun autre coût ou frais horaires supplémentaires pour le reste de la réservation, quel que soit le nombre d'heures utilisé.
- Frais initiaux partiels : une partie du coût doit être payée au départ et les heures restantes pendant la période sont facturées à un tarif horaire réduit, que la Instance réservée soit utilisée ou non.
- Sans frais initiaux : vous devez régler un taux horaire avec remise pour chaque heure entrant dans le cadre de l'abonnement, que la Instance réservée soit utilisée ou non. Aucun paiement initial n'est requis.

 Note

Les instances réservées sans frais initiaux sont basées sur une obligation contractuelle d'effectuer des paiements mensuels pendant toute la durée de la réservation. C'est la raison pour laquelle il est nécessaire de fournir un bon historique de facturation pour pouvoir acheter des instances réservées sans frais initiaux.

En règle générale, l'option la plus économique consiste à acheter des instances réservées en versant un paiement initial plus élevé. Vous pouvez aussi trouver des instances réservées proposées par des vendeurs tiers à des prix inférieurs avec des durées de paiement plus courtes sur la marketplace des instances réservées. Pour plus d'informations, consultez [Vendre sur la marketplace des instances réservées](#).

Classe d'offre

Si vos besoins informatiques évoluent, vous pourrez probablement modifier ou échanger votre Instance réservée, en fonction de la classe d'offre.

- Standard : proposent la réduction la plus importante, mais ne peut que se modifier. Les instances réservées Standard ne peuvent pas être échangées.
- Convertible : proposent une réduction plus faible que les Instances réservées Standard, mais peut s'échanger contre une Instance réservée convertible avec différents attributs d'instance. Les instances réservées convertibles peuvent également être modifiées.

Pour plus d'informations, consultez [Types d'instances réservées \(classes d'offres\)](#).

 Important

Une fois que vous avez acheté une Instance réservée, vous ne pouvez pas annuler votre achat. Toutefois, vous pourrez probablement [modifier](#), [échanger](#) ou [vendre](#) votre Instance réservée si vos besoins évoluent.

Pour de plus informations, consultez la [page relative à la tarification des instances réservées Amazon EC2](#).

instances réservées régionales et zonales (portée)

Lorsque vous achetez une Instance réservée, vous déterminez la portée de la Instance réservée. La portée est régionale ou zonale.

- Régionale : lorsque vous achetez une Instance réservée pour une région, elle est appelée Instance réservée régionale.
- Zonale : lorsque vous achetez une Instance réservée pour une Zone de disponibilité spécifique, il s'agit d'une Instance réservée zonale.

L'étendue n'affecte pas le prix. Vous payez le même prix pour un Instance réservée régional ou zonal. Pour plus d'informations sur la tarification Instance réservée, consultez [Variables clés déterminant la tarification d'une Instance réservée](#) et [Tarification des instances réservées Amazon EC2](#).

Pour plus d'informations sur la façon de spécifier la portée d'une instance réservée, consultez [Attributs RI](#), plus précisément le point Zone de disponibilité.

Différences entre les instances réservées régionales et zonales

Le tableau suivant souligne certaines différences essentielles entre les instances réservées zonales et les instances réservées régionales :

	instances réservées régionales	instances réservées zonales
Possibilité de réserver de la capacité	Une Instance réservée de région ne réserve pas de capacité.	Une Instance réservée de zone réserve de la capacité dans la zone de disponibilité spécifiée.
Flexibilité des zones de disponibilité	La remise de Instance réservée s'applique à l'utilisation d'une instance dans n'importe quelle zone de disponibilité de la région spécifiée.	Aucune flexibilité de zone de disponibilité—la remise de Instance réservée s'applique à l'utilisation d'instance uniquement dans la zone de disponibilité spécifiée.

	instances réservées régionale s	instances réservées zonales
Flexibilité de la taille de l'instance	<p>La remise Instance réservée s'applique à une utilisation d'instance, quelle que soit la taille, au sein de cette famille d'instances.</p> <p>Prise en charge uniquement sur les instances réservées Amazon Linux/Unix avec location par défaut. Pour plus d'informations, consultez Flexibilité de taille d'instance déterminée par le facteur de normalisation.</p>	<p>Aucune flexibilité de taille d'instance—la remise de Instance réservée s'applique pour l'utilisation d'instance uniquement pour la taille et le type d'instance spécifiés.</p>
Mise en file d'attente d'un achat	<p>Vous pouvez mettre en file d'attente les achats pour les instances réservées régionale s.</p>	<p>Vous ne pouvez pas mettre en file d'attente les achats pour les instances réservées zonales.</p>

Pour plus d'informations et d'exemples, consultez [Application des instances réservées](#).

Types d'instances réservées (classes d'offres)

La classe d'offre d'une Instance réservée est Standard ou Convertible. Une Instance réservée Standard offre un rabais plus important qu'une Instance réservée Convertible, mais vous ne pouvez pas échanger une Instance réservée Standard. Vous pouvez échanger les instances réservées Convertible. Vous pouvez modifier les instances réservées Standard et Convertible.

La configuration d'une Instance réservée comprend un type d'instance unique, une plateforme, une étendue et une location pendant une période donnée. Si vos besoins informatiques changent, vous pourriez être en mesure de modifier ou d'échanger votre Instance réservée.

Différences entre les instances réservées Standard et Convertible

Les différences entre les instances réservées Convertible et Standard sont les suivantes.

	Instance réservée standard	Instance réservée convertible
Modifier instances réservées	Certains attributs peuvent être modifiés. Pour plus d'informations, consultez Modifier instances réservées .	Certains attributs peuvent être modifiés. Pour plus d'informations, consultez Modifier instances réservées .
Échanger des instances réservées	Ne peut pas être échangée.	Peut être échangée, pendant la période de paiement, contre une autre Instance réservée convertible avec de nouveaux attributs tels que la famille de l'instance, le type d'instance, la plateforme, l'étendue ou la location. Pour plus d'informations, consultez Échanger des instances réservées convertibles .
Vendre sur la marketplace des instances réservées	Peut être vendue sur la marketplace des instances réservées.	Ne peut pas être vendue sur la marketplace des instances réservées.
Acheter sur la marketplace des instances réservées	Peut être achetée sur la marketplace des instances réservées.	Ne peut pas être achetée sur la marketplace des instances réservées.

Application des instances réservées

Les instances réservées ne sont pas des instances physiques, mais correspondent à une remise de facturation appliquée à l'exécution d'instances à la demande dans votre compte. Les instances à la demande doivent correspondre à certains attributs des instances réservées pour bénéficier de la remise de facturation.

Si vous achetez une instance réservée et que vous avez déjà une instance à la demande en cours d'exécution qui correspond aux attributs de l'instance réservée, la remise de facturation est immédiatement et automatiquement appliquée. Vous n'avez pas besoin de redémarrer vos instances. Si vous n'avez pas d'instance à la demande éligible en cours d'exécution, lancez une instance à la demande ayant les mêmes attributs que votre instance réservée. Pour plus d'informations, consultez [Utiliser votre instances réservées](#).

La classe d'offre (Standard ou Convertible) de l'instance réservée n'affecte pas la façon dont la remise de facturation est appliquée.

Rubriques

- [Application des instances réservées zonales](#)
- [Application des instances réservées régionales](#)
- [Flexibilité de la taille de l'instance](#)
- [Exemples d'application des instances réservées](#)

Application des instances réservées zonales

Une instance réservée achetée pour réserver une capacité dans une zone de disponibilité spécifique est appelée instance réservée de zone.

- La remise d'instance réservée s'applique à l'utilisation correspondante d'une instance dans cette zone de disponibilité.
- Les attributs (location, plateforme, zone de disponibilité, type d'instance et taille d'instance) des instances en cours d'exécution doivent correspondre à celles des instances réservées.

Par exemple, si vous achetez deux instances réservées standard Linux/Unix à location par défaut `c4.xlarge` dans la zone de disponibilité `us-east-1a`, jusqu'à deux instances Linux/Unix à location par défaut `c4.xlarge` s'exécutant dans la zone de disponibilité `us-east-1a` peuvent bénéficier de la remise d'instance réservée.

Application des instances réservées régionales

Une instance réservée achetée pour une région est appelée instance réservée régionale et assure une flexibilité de zone de disponibilité et de taille d'instance.

- La remise de Instance réservée s'applique à l'utilisation d'une instance dans n'importe quelle zone de disponibilité de la région spécifiée.

- La remise d'instance réservée s'applique à une utilisation d'instance, quelle que soit la taille, au sein de cette famille d'instances. Il s'agit de la [flexibilité de la taille d'instance](#).

Flexibilité de la taille de l'instance

Avec la flexibilité de la taille d'instance, la remise d'instance réservée s'applique à une utilisation d'instances de la même [famille, génération et du même attribut](#). L'instance réservée est appliquée de la taille d'instance la plus petite à la taille d'instance la plus grande au sein de la famille de l'instance, en fonction du facteur de normalisation. Pour voir un exemple d'application de la réduction sur les instances réservées, consultez [Scénario 2 : instances réservées dans un compte unique utilisant le facteur de normalisation](#).

Limites

- Prise en charge : la flexibilité de la taille des instances n'est prise en charge que pour les instances réservées régionales.
- Pas de prise en charge : la flexibilité de la taille des instances n'est pas prise en charge pour les instances réservées suivantes :
 - Les instances réservées achetées pour une Zone de disponibilité spécifique (instances réservées zonales)
 - Instances réservées pour les instances G4ad, G4dn, G5, G5g, Inf1 et Inf2
 - instances réservées pour Windows Server, Windows Server avec SQL Standard, Windows Server avec SQL Server Enterprise, Windows Server avec SQL Server Web, RHEL et SUSE Linux Enterprise Server
 - instances réservées avec location dédiée

Flexibilité de taille d'instance déterminée par le facteur de normalisation

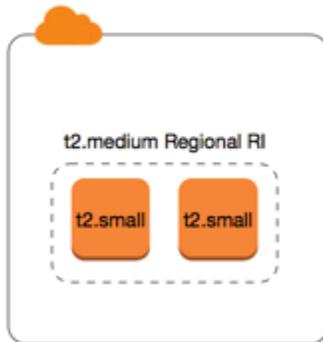
La flexibilité de la taille d'instance est déterminée par le facteur de normalisation de la taille d'instance. La remise s'applique complètement ou partiellement aux instances en cours d'exécution d'une même famille de l'instance, en fonction de la taille d'instance de la réservation, dans n'importe quelle zone de disponibilité de la région. Les seuls attributs qui doivent correspondre sont la famille de l'instance, la location et la plate-forme.

Le tableau suivant décrit les différentes tailles au sein d'une famille de l'instance et le facteur de normalisation correspondant. Cette échelle est utilisée pour appliquer le taux avec remise des instances réservées à l'utilisation normalisée de la famille de l'instance.

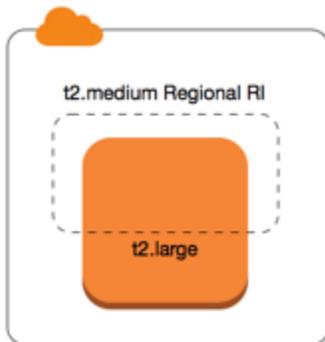
Taille d'instance	Facteur de normalisation
nano	0.25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448

Taille d'instance	Facteur de normalisation
112xlarge	896

Par exemple, le facteur de normalisation d'une instance `t2.medium` est 2. Si vous achetez une Instance réservée Amazon Linux/Unix `t2.medium` à location par défaut dans la région US East (N. Virginia) et que vous avez deux instances `t2.small` en cours d'exécution dans votre compte dans cette région, l'avantage de facturation est appliqué entièrement à ces deux instances.



Si vous avez une instance `t2.large` en cours d'exécution dans votre compte dans la région US East (N. Virginia), l'avantage de facturation est appliqué à 50 % de l'utilisation de l'instance.



Le facteur de normalisation est également appliqué lors de la modification d'instances réservées standard. Pour plus d'informations, consultez [Modifier instances réservées](#).

Facteur de normalisation pour les instances matériel nu

La flexibilité de taille d'instance s'applique également aux instances à matériel nu dans la famille d'instances. Si vous disposez de instances réservées Amazon Linux/Unix régionales avec une location partagée sur des instances à matériel nu, vous pouvez profiter des économies Instance réservée avec la même famille d'instances. L'inverse est également vrai : si vous disposez de

instances réservées Amazon Linux/Unix régionales avec une location partagée sur des instances de la même famille que l'instance à matériel nu, vous pouvez profiter des économies Instance réservée sur l'instance à matériel nu.

La taille d'instances `metal` ne dispose pas d'un seul et unique facteur de normalisation. Une instance bare metal a le même facteur de normalisation que la taille d'instance virtualisée équivalente au sein de la même famille de l'instance. Par exemple, une instance `i3.metal` a le même facteur de normalisation qu'une instance `i3.16xlarge`.

Taille d'instance	Facteur de normalisation
<code>a1.metal</code>	32
<code>m5zn.metal</code> <code>x2iezn.metal</code> <code>z1d.metal</code>	96
<code>c6g.metal</code> <code>c6gd.metal</code> <code>i3.metal</code> <code>m6g.metal</code> <code>m6gd.metal</code> <code>r6g.metal</code> <code>r6gd.metal</code> <code>x2gd.metal</code>	128
<code>c5n.metal</code>	144
<code>c5.metal</code> <code>c5d.metal</code> <code>i3en.metal</code> <code>m5.metal</code> <code>m5d.metal</code> <code>m5dn.metal</code> <code>m5n.metal</code> <code>r5.metal</code> <code>r5b.metal</code> <code>r5d.metal</code> <code>r5dn.metal</code> <code>r5n.metal</code>	192
<code>c6i.metal</code> <code>c6id.metal</code> <code>m6i.metal</code> <code>m6id.metal</code> <code>r6d.metal</code> <code>r6id.metal</code>	256
<code>u-*.metal</code>	896

Par exemple, une instance `i3.metal` dispose d'un facteur de normalisation de 128. Si vous achetez un Instance réservée Amazon Linux/Unix à location par défaut `i3.metal` dans la US East (N. Virginia), l'avantage de facturation peut s'appliquer comme suit :

- Si vous disposez d'une `i3.16xlarge` en cours d'exécution dans votre compte pour cette région, l'avantage de facturation peut s'appliquer entièrement à l'instance `i3.16xlarge` (facteur de normalisation `i3.16xlarge` = 128).

- Sinon, si vous disposez de deux instances `i3.8xlarge` en cours d'exécution dans votre compte pour cette région, l'avantage de facturation peut s'appliquer entièrement aux deux instances `i3.8xlarge` (facteur de normalisation `i3.8xlarge` = 64).
- Sinon, si vous disposez de quatre instances `i3.4xlarge` en cours d'exécution dans votre compte pour cette région, l'avantage de facturation peut s'appliquer entièrement aux quatre instances `i3.4xlarge` (facteur de normalisation `i3.4xlarge` = 32).

L'inverse est également vrai. Par exemple, si vous achetez deux Instances réservées Amazon Linux/Unix à location par défaut `i3.8xlarge` dans la US East (N. Virginia) et que vous disposez d'une instance `i3.metal` dans cette région, l'avantage de facturation s'applique entièrement à l'instance `i3.metal`.

Exemples d'application des instances réservées

Les scénarios suivants couvrent les façons dont les instances réservées sont appliquées.

- [Scénario 1 : instances réservées dans un compte unique](#)
- [Scénario 2 : instances réservées dans un compte unique utilisant le facteur de normalisation](#)
- [Scénario 3 : instances réservées régionales dans des comptes liés](#)
- [Scénario 4 : instances réservées zonales dans un compte lié](#)

Scénario 1 : instances réservées dans un compte unique

Vous exécutez les instances à la demande suivantes dans le compte A :

- 4 instances `m3.large` Linux à location par défaut dans la zone de disponibilité `us-east-1a`
- 2 instances `m4.xlarge` Amazon Linux à location par défaut dans la zone de disponibilité `us-east-1b`
- 1 instance Amazon Linux `c4.xlarge` à location par défaut dans la zone de disponibilité `us-east-1c`

Vous achetez ensuite les instances réservées suivantes dans le compte A :

- 4 Instances réservées `m3.large` Linux à location par défaut dans la zone de disponibilité `us-east-1a` (la capacité est réservée)
- 4 Instances réservées Amazon Linux `m4.large` à location par défaut dans la région `us-east-1`
- 1 Instances réservées Amazon Linux `c4.large` à location par défaut dans la région `us-east-1`

Les avantages de l'Instance réservée sont appliqués de la façon suivante :

- La remise et la réservation de capacité des quatre Instances réservées zonales `m3.large` sont utilisées par les quatre instances `m3.large`, car leurs attributs (taille de l'instance, région, plateforme, location) correspondent.
- Les Instances réservées régionales `m4.large` fournissent une flexibilité de zone de disponibilité et de taille d'instance, car il s'agit d'Instances réservées Amazon Linux régionales à location par défaut.

Une instance `m4.large` est équivalente à 4 unités normalisées/heure.

Vous avez acheté quatre Instances réservées régionales `m4.large` et, au total, celles-ci sont égales à 16 unités normalisées/heure (4x4). Le compte A comporte deux instances `m4.xlarge` en cours d'exécution, ce qui est équivalent à 16 unités normalisées/heure (2x8). Dans ce cas, les quatre instances réservées régionales `m4.large` apportent l'avantage de facturation complet à l'utilisation des deux instances `m4.xlarge`.

- L'Instance réservée régionale `c4.large` dans la région `us-east-1` fournit une flexibilité de zone de disponibilité et de taille d'instance, car il s'agit d'une Instance réservée régionale Amazon Linux à location par défaut et elle s'applique à l'instance `c4.xlarge`. Une instance `c4.large` est équivalente à 4 unités normalisées/heure et une instance `c4.xlarge` est équivalente à 8 unités normalisées/heure.

Dans ce cas, l'Instance réservée régionale `c4.large` apporte un avantage partiel à l'utilisation de `c4.xlarge`. Cela est dû au fait qu'une Instance réservée `c4.large` est équivalente à 4 unités normalisées/heure d'utilisation, mais qu'une instance `c4.xlarge` requiert 8 unités normalisées/heure. Par conséquent, la remise de facturation de l'Instance réservée `c4.large` s'applique à 50 % de l'utilisation de `c4.xlarge`. L'utilisation `c4.xlarge` restante est facturée au taux à la demande.

Scénario 2 : instances réservées dans un compte unique utilisant le facteur de normalisation

Vous exécutez les instances à la demande suivantes dans le compte A :

- 2 instances `m3.xlarge` Amazon Linux à location par défaut dans la zone de disponibilité `us-east-1a`
- 2 instances `m3.large` Amazon Linux à location par défaut dans la zone de disponibilité `us-east-1b`

Vous achetez ensuite l'instance réservée suivante dans le compte A :

- 1 instance réservée Amazon Linux m3.2xlarge à location par défaut dans la région us-east-1

Les avantages de l'Instance réservée sont appliqués de la façon suivante :

- L'instance réservée régionale m3.2xlarge dans la région us-east-1 fournit une flexibilité de zone de disponibilité et de taille d'instance, car il s'agit d'une instance réservée régionale Amazon Linux à location par défaut. Elle s'applique d'abord aux instances m3.large, puis aux instances m3.xlarge, car elle s'applique de la taille d'instance la plus petite à la taille d'instance la plus grande au sein de la famille de l'instance, en fonction du facteur de normalisation.

Une instance m3.large est équivalente à 4 unités normalisées/heure.

Une instance m3.xlarge est équivalente à 8 unités normalisées/heure.

Une instance m3.2xlarge est équivalente à 16 unités normalisées/heure.

L'avantage est appliqué comme suit :

L'instance réservée régionale m3.2xlarge offre un avantage complet pour l'utilisation de deux instances m3.large, car ensemble, ces instances représentent 8 unités normalisées/heure. Ainsi, il reste 8 unités normalisées/heure à appliquer aux instances m3.xlarge.

Avec les 8 unités normalisées/heure restantes, l'instance réservée régionale m3.2xlarge offre un avantage complet pour l'utilisation d'une instance m3.xlarge, car chaque instance m3.xlarge est équivalente à 8 unités normalisées/heure. L'utilisation m3.xlarge restante est facturée au taux à la demande.

Scénario 3 : instances réservées régionales dans des comptes liés

Les instances réservées sont d'abord appliquées à une utilisation au sein du compte d'achat, puis à l'utilisation éligible dans tout autre compte au sein de l'organisation. Pour plus d'informations, consultez [instances réservées et la facturation consolidée](#). Pour les instances réservées régionales qui offrent la flexibilité de la taille d'instance, l'avantage est appliqué de la taille d'instance la plus petite à la taille d'instance la plus grande au sein de la famille de l'instance.

Vous exécutez les instances à la demande suivantes dans le compte A (le compte d'achat) :

- 2 instances m4.xlarge Linux à location par défaut dans la zone de disponibilité us-east-1a

- 1 instances `m4.2xlarge` Linux à location par défaut dans la zone de disponibilité `us-east-1b`
- 2 instances `c4.xlarge` Linux à location par défaut dans la zone de disponibilité `us-east-1a`
- 1 instances `c4.2xlarge` Linux à location par défaut dans la zone de disponibilité `us-east-1b`

Un autre client exécute les instances à la demande suivantes dans le compte B (un compte lié) :

- 2 instances `m4.xlarge` Linux à location par défaut dans la zone de disponibilité `us-east-1a`

Vous achetez ensuite les instances réservées régionales suivantes dans le compte A :

- 4 Instances réservées Linux `m4.xlarge` à location par défaut dans la région `us-east-1`
- 2 Instances réservées Linux `c4.xlarge` à location par défaut dans la région `us-east-1`

Les avantages de l'Instance réservée régionale sont appliqués de la façon suivante :

- La remise des quatre Instances réservées `m4.xlarge` est utilisée par les deux instances `m4.xlarge` et par l'instance `m4.2xlarge` unique dans le compte A (compte d'achat). Les trois instances correspondent toutes aux attributs (famille de l'instance, région, plate-forme, location). La remise s'applique d'abord aux instances dans le compte d'achat (compte A), même si le compte B (compte lié) dispose de deux `m4.xlarge` qui correspondent également aux Instances réservées. Il n'y a pas de réservation de capacité, car les instances réservées sont des instances réservées régionales.
- La remise des deux Instances réservées `c4.xlarge` s'applique aux deux instances `c4.xlarge`, car elles ont une taille d'instance plus petite que l'instance `c4.2xlarge`. Il n'y a pas de réservation de capacité, car les instances réservées sont des instances réservées régionales.

Scénario 4 : instances réservées zonales dans un compte lié

En général, les instances réservées appartenant à un compte sont appliquées en premier à l'utilisation dans ce compte. Cependant, s'il existe des instances réservées éligibles non utilisées pour une zone de disponibilité spécifique (instances réservées zonales) dans d'autres comptes de l'organisation, elles sont appliquées au compte avant les instances réservées régionales appartenant au compte. Ceci vise à garantir une utilisation maximale des Instance réservée et une facture moins élevée. A des fins de facturation, tous les comptes de l'organisation sont traités comme s'il s'agissait d'un seul compte. L'exemple suivant peut contribuer à en apporter l'explication.

Vous exécutez l'instance à la demande suivante dans le compte A (le compte d'achat) :

- 1 instance m4.xlarge Linux à location par défaut dans la zone de disponibilité us-east-1a

Un client exécute l'instance à la demande suivante dans le compte B lié :

- 1 instance m4.xlarge Linux à location par défaut dans la zone de disponibilité us-east-1b

Vous achetez ensuite les instances réservées régionales suivantes dans le compte A :

- 1 Instance réservée Linux m4.xlarge à location par défaut dans la région us-east-1

Un client achète également les instances réservées zonales suivantes dans le compte C lié :

- 1 Instances réservées m4.xlarge Linux à location par défaut dans la zone de disponibilité us-east-1a

Les avantages de l'Instance réservée sont appliqués de la façon suivante :

- La remise de l'Instance réservée zonale m4.xlarge appartenant au compte C est appliquée à l'utilisation de m4.xlarge dans le compte A.
- La remise de l'Instance réservée régionale m4.xlarge appartenant au compte A est appliquée à l'utilisation de m4.xlarge dans le compte B.
- Si l'Instance réservée régionale appartenant au compte A est appliquée d'abord à l'utilisation dans le compte A, l'Instance réservée zonale appartenant au compte C reste inutilisée et l'utilisation dans le compte B est facturée aux tarifs à la demande.

Pour plus d'informations, consultez [Instances réservées dans le rapport Billing and Cost Management](#).

Note

Les instances réservées zonales réservent de la capacité uniquement au compte propriétaire et ne peuvent pas être partagées avec d'autres Comptes AWS. Si vous devez partager la capacité avec d'autres Comptes AWS, utilisez [On-Demand Capacity Reservations](#).

Utiliser votre instances réservées

Les instances réservées sont appliquées automatiquement aux instances à la demande en cours d'exécution correspondant aux spécifications. Si vous n'avez pas d'instances à la demande en cours d'exécution qui correspond aux spécifications de votre Instance réservée, l'Instance réservée est inutilisée jusqu'à ce que vous lanciez une instance avec les spécifications requises.

Si vous lancez une instance à la demande pour bénéficier de l'avantage de facturation d'une instance réservée, veuillez à spécifier les informations suivantes lors de la configuration.

Plateforme

Vous devez spécifier une Amazon Machine Image (AMI) qui correspond à la plateforme (description du produit) de votre instance réservée. Par exemple, si vous avez spécifié Linux/UNIX pour votre instance réservée, vous pouvez lancer une instance à partir d'une AMI Amazon Linux ou d'une AMI Ubuntu.

Type d'instance

Si vous avez acheté une instance réservée zonale, vous devez spécifier le même type d'instance que pour votre instance réservée ; par exemple, `t3.large`. Pour plus d'informations, consultez [Application des instances réservées zonales](#).

Si vous avez acheté une instance réservée régionale, vous devez spécifier un type d'instance de la même famille d'instances que le type d'instance de votre instance réservée. Par exemple, si vous avez spécifié `t3.xlarge` pour votre instance réservée, vous devez lancer votre instance à partir de la famille T3, mais vous pouvez spécifier n'importe quelle taille, par exemple, `t3.medium`. Pour plus d'informations, consultez [Application des instances réservées régionales](#).

Zone de disponibilité

Si vous avez acheté une instance réservée zonale pour une zone de disponibilité spécifique, vous devez lancer l'instance dans la même zone de disponibilité.

Si vous avez acheté une instance réservée régionale, vous pouvez lancer l'instance dans n'importe quelle zone de disponibilité de la région spécifiée pour l'instance réservée.

Location

La location (`dedicated` ou `shared`) de votre instance doit correspondre à celle de l'instance réservée. Pour plus d'informations, consultez [Dedicated instances](#).

Pour voir des exemples d'application des instances réservées à vos instances à la demande en cours d'exécution, consultez [Application des instances réservées](#). Pour plus d'informations, consultez [Pourquoi mes instances réservées Amazon EC2 ne s'appliquent-elles pas à ma AWS facturation comme prévu ?](#)

Vous pouvez utiliser diverses méthodes pour lancer les instances à la demande qui utilisent votre remise d'instance réservée. Pour plus d'informations sur les différentes méthodes de lancement, consultez [Lancer votre instance](#). Vous pouvez également utiliser Amazon EC2 Auto Scaling pour lancer une instance. Pour plus d'informations, consultez le [Guide de l'utilisateur Amazon EC2 Auto Scaling](#).

Principes de facturation

Toutes les instances réservées vous permettent de bénéficier d'une remise par rapport à la tarification à la demande. Avec les instances réservées, vous payez pour toute la durée de l'abonnement et non en fonction de l'utilisation réelle. Vous pouvez choisir d'effectuer un paiement initial ou un paiement initial partiel, ou mensuel pour votre Instance réservée, en fonction de l'[option de paiement](#) spécifiée pour l'Instance réservée.

Lorsque des instances réservées expirent, le tarif à la demande est facturé pour l'utilisation d'instance EC2. Vous pouvez mettre en file d'attente l'achat d'une Instance réservée jusqu'à trois ans en avance. Cela peut vous aider à garantir une couverture ininterrompue. Pour plus d'informations, consultez [Mettre votre achat en file d'attente](#).

Le niveau AWS gratuit est disponible pour les nouveaux AWS comptes. Si vous avez recours à l'offre gratuite AWS pour exécuter les instances Amazon EC2 et que vous achetez ensuite une instance réservée, vous serez facturé conformément aux règles de tarification standard. Pour plus d'informations, consultez [Offre gratuite AWS](#).

Sommaire

- [Facturation de l'utilisation](#)
- [Affichage d'une facture](#)
- [instances réservées et la facturation consolidée](#)
- [Niveaux de tarification avec remise d'Instance réservée](#)

Facturation de l'utilisation

Les instances réservées sont facturées toutes les heures d'horloge au cours de la réservation sélectionnée, que l'instance soit exécutée. Chaque heure d'horloge commence à l'heure (zéro minute et zéro seconde après l'heure) d'une horloge standard de 24 heures. Par exemple, 1:00:00 à 1:59:59 est une heure horloge. Pour plus d'informations sur les états de l'instance, consultez [Cycle de vie d'une instance](#).

L'avantage de facturation d'une Instance réservée peut être appliqué à une instance en cours d'exécution sur une base par seconde. La facturation par seconde est disponible pour les instances qui utilisent une distribution Linux en open source, telle que Amazon Linux et Ubuntu. La facturation par heure est utilisée pour les distributions Linux commerciales, telles que Red Hat Enterprise Linux et SUSE Linux Enterprise Server.

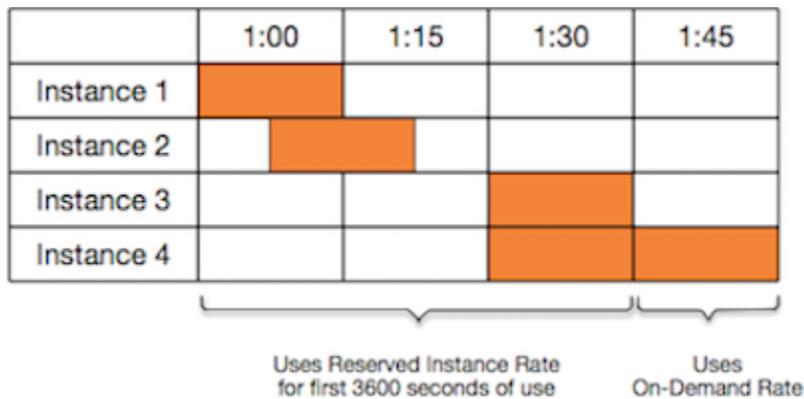
L'avantage de facturation d'une Instance réservée peut s'appliquer à un maximum de 3 600 secondes (une heure) d'utilisation d'instance par heure d'horloge. Vous pouvez exécuter plusieurs instances simultanément, mais vous ne pouvez bénéficier de l'avantage de la remise d'Instance réservée que pour un total de 3600 secondes par heure d'horloge ; l'utilisation d'instance qui dépasse 3600 secondes dans une heure d'horloge est facturée au tarif à la demande.

Par exemple, si vous achetez une Instance réservée `m4.xlarge` et que vous exécutez simultanément quatre instances `m4.xlarge` pendant une heure, une instance est facturée au tarif d'une heure d'utilisation d'Instance réservée et les trois autres instances sont facturées au tarif de trois heures d'utilisation à la demande.

Par contre, si vous achetez une Instance réservée `m4.xlarge` et que vous exécutez simultanément quatre instances `m4.xlarge` pendant 15 minutes (900 secondes), chacune au cours de la même heure, la durée d'exécution totale pour les instances est d'une heure, ce qui se traduit par une heure d'utilisation d'Instance réservée et 0 heure d'utilisation à la demande.

	1:00	1:15	1:30	1:45
Instance 1				
Instance 2				
Instance 3				
Instance 4				

Si plusieurs instances éligibles s'exécutent simultanément, l'avantage de facturation d'Instance réservée est appliqué à toutes les instances en même temps pour un maximum de 3600 secondes dans une heure d'horloge ; ensuite ce sont les tarifs à la demande qui s'appliquent.



Cost Explorer dans la console [Billing and Cost Management](#) vous permet d'analyser les économies réalisées par rapport à l'exécution d'Instances à la demande. Le [questions fréquentes \(FAQ\) Instances réservées](#) inclut un exemple de calcul de valeur de liste.

Si vous fermez votre AWS compte, la facturation à la demande de vos ressources cesse. Toutefois, si vous avez des instances réservées dans votre compte, vous continuez à recevoir une facture pour ces instances jusqu'à ce qu'elles expirent.

Affichage d'une facture

Vous pouvez consulter les frais et tarifs appliqués à votre compte sur la page de la console [AWS Billing and Cost Management](#).

- Le Tableau de bord affiche un récapitulatif des dépenses de votre compte.
- Sur la page Factures, sous Détails, développez la section Elastic Compute Cloud et la région pour obtenir des informations de facturation sur vos Instances réservées.

Vous pouvez consulter les frais en ligne ou télécharger un fichier CSV.

Vous pouvez également suivre l'utilisation de vos instances réservées à l'aide du rapport sur les AWS coûts et l'utilisation. Pour plus d'informations, consultez [Instances réservées](#) dans le rapport d'utilisation et de coût du Guide de l'utilisateur AWS Billing .

instances réservées et la facturation consolidée

Les avantages de tarification des instances réservées sont partagés lorsque le compte d'achat fait partie d'un ensemble de comptes facturés réunis sous un même compte payeur de facturation consolidée. L'utilisation d'instance pour tous les comptes membres est regroupé dans le compte souscripteur tous les mois. Cette fonctionnalité est généralement utile dans le cadre des sociétés

disposant de plusieurs équipes ou groupes fonctionnels. Ensuite, la logique standard des Instance réservées est appliquée pour calculer le montant de la facture. Pour plus d'informations, consultez [Facturation consolidée dans le AWS Organizations](#).

Si vous fermez le compte qui a acheté l'Instance réservée, le compte payeur est débité pour l'Instance réservée jusqu'à ce que celle-ci expire. Le compte fermé est supprimé définitivement après 90 jours, et les comptes membres ne bénéficient plus de la réduction de facturation pour Instance réservée.

Note

Les instances réservées zonales réservent de la capacité uniquement au compte propriétaire et ne peuvent pas être partagées avec d'autres Comptes AWS. Si vous devez partager la capacité avec d'autres Comptes AWS, utilisez [On-Demand Capacity Reservations](#).

Niveaux de tarification avec remise d'Instance réservée

Si votre compte est éligible pour bénéficier d'un niveau de tarification avec remise, il bénéficie automatiquement des remises dès le départ et le tarif d'utilisation des instances pour tous les achats d'Instance réservée effectués dans le cadre de ce niveau à partir de ce moment-là. Pour que votre compte soit éligible, la valeur de la liste répertoriant vos instances réservées dans la région doit s'élever à 500 000 USD au minimum.

Les règles suivantes s'appliquent :

- Les niveaux de tarification et les remises associées s'appliquent uniquement aux achats d'instances réservées standard Amazon EC2.
- Les niveaux de tarification ne s'appliquent pas aux instances réservées pour Windows avec SQL Server Standard, SQL Server Web et SQL Server Enterprise.
- Les niveaux de tarification ne s'appliquent pas aux instances réservées pour Linux avec SQL Server Standard, SQL Server Web et SQL Server Enterprise.
- Les remises tarifaires s'appliquent uniquement aux achats effectués auprès de AWS. Elles ne s'appliquent pas aux achats d'instances réservées tierces.
- Les achats d'Instance réservée convertible ne bénéficient pas actuellement de niveaux de tarification avec remise.

Rubriques

- [Calculer les remises de tarification d'une Instance réservée](#)
- [Acheter avec un niveau de remise](#)
- [Changement de niveau de tarification](#)
- [Facturation consolidée pour les niveaux de tarification](#)

Calculer les remises de tarification d'une Instance réservée

Vous pouvez déterminer le niveau de tarification de votre compte en calculant la valeur de la liste répertoriant toutes vos instances réservées dans une région. Multipliez le taux horaire récurrent de chaque réservation par le nombre total d'heures pour l'abonnement et ajoutez le tarif initial avant remise (également connu sous le nom de tarif fixe) au moment de l'achat. Dans la mesure où la valeur de la liste repose sur le tarif avant remise (public), elle ne change pas si vous êtes éligible pour une remise sur le volume ou si le tarif chute une fois que vous avez acheté vos instances réservées.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Par exemple, pour une Instance réservée `t2.small` avec frais initiaux partiels d'une année, supposons que le prix initial est de 60,00 USD et que le tarif horaire est de 0,007 USD. Cela donne une valeur de liste de 121,32 USD.

```
121.32 = 60.00 + (0.007 * 8760)
```

New console

Pour afficher les valeurs du tarif fixe des instances réservées à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Reserved Instances (Instances réservées).
3. Pour afficher la colonne du prix initial, choisissez settings



) dans le coin supérieur droit, activez le prix initial et choisissez Confirmer.

Old console

Pour afficher les valeurs du tarif fixe des instances réservées à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, choisissez Reserved Instances (Instances réservées).
3. Pour afficher la colonne Prix initial, choisissez settings



) dans le coin supérieur droit, sélectionnez Prix initial, puis cliquez sur Fermer.

Pour afficher les valeurs du tarif fixe des instances réservées à l'aide de la ligne de commande

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (AWS Tools for Windows PowerShell)
- [DescribeReservedInstances](#) (API Amazon EC2)

Acheter avec un niveau de remise

Lorsque vous achetez des instances réservées, Amazon EC2 applique automatiquement les remises à la partie de votre achat se trouvant au niveau de la tarification avec remise. Vous ne devez rien faire de particulier et vous pouvez acheter des instances réservées à l'aide de n'importe quel outil Amazon EC2. Pour plus d'informations, consultez [Acheter des instances réservées](#).

Une fois que la valeur de la liste répertoriant vos instances réservées actives dans une région a atteint le niveau de tarification avec remise, tous les achats suivants d'instances réservées dans cette région sont facturés au tarif réduit. Si un seul achat d'instances réservées dans une région vous permet de dépasser le seuil d'un niveau de remise, la partie de l'achat qui dépasse ce seuil est facturée au tarif réduit. Pour plus d'informations sur les ID temporaires d'Instance réservée qui sont créés au cours du processus d'achat, consultez [Changement de niveau de tarification](#).

Si votre valeur de liste tombe en dessous du seuil minimum pour ce niveau de tarification avec remise (par exemple, lorsque certaines instances réservées arrivent à expiration), les achats suivants d'instances réservées dans la région ne sont pas facturés au tarif réduit. Toutefois, vous continuez à bénéficier de la remise appliquée aux instances réservées initialement achetées dans le cadre du niveau de tarification avec remise.

Lorsque vous achetez des instances réservées, quatre scénarios peuvent se produire :

- Aucune remise : votre achat dans une région se trouve toujours en dessous du seuil de remise.
- Remise partielle : votre achat dans une région dépasse le seuil du premier niveau de tarification avec remise. Aucune remise n'est appliquée à une ou plusieurs réservations et le taux avec remise est appliqué aux réservations restantes.

- **Remise complète** : tous vos achats au sein d'une région relèvent d'un niveau de tarification avec remise et sont en conséquence facturés au tarif réduit.
- **Deux taux avec remise** : votre achat dans une région vous permet de passer d'un niveau de tarification inférieur avec remise à un niveau de tarification supérieur avec remise. Deux taux différents sont facturés : une ou plusieurs réservations au taux avec remise inférieur et les réservations restantes au taux avec remise supérieur.

Changement de niveau de tarification

Si votre achat vous fait passer à un niveau de tarification avec remise, vous voyez plusieurs entrées pour cet achat : une première correspondant à la partie de l'achat facturée au prix standard et une deuxième correspondant à la partie de l'achat facturée au taux avec remise applicable.

Le service des Instance réservée génère plusieurs ID d'Instance réservée dans la mesure où votre achat vous permet de passer à un niveau avec remise ou d'un niveau avec remise inférieur à un niveau avec remise supérieur. Un ID est attribué à chaque ensemble de réservations d'un niveau. C'est pourquoi l'ID retourné par la commande CLI ou l'action d'API correspondant à votre achat est différent du véritable ID des nouvelles instances réservées.

Facturation consolidée pour les niveaux de tarification

Un compte de facturation consolidée regroupe la valeur de liste des comptes membres au sein d'une région. Lorsque la valeur de la liste de toutes les instances réservées actives du compte de facturation consolidée atteint un niveau de tarification avec remise, toute instances réservées achetée après ce stade par un membre du compte de facturation consolidée est facturée au tarif avec remise (tant que la valeur de la liste associée à ce compte consolidé reste au-dessus du seuil du niveau de tarification avec remise). Pour plus d'informations, consultez [instances réservées et la facturation consolidée](#).

Acheter des instances réservées

Pour acheter une instance réservée, recherchez les offres d'instances réservées proposées par des vendeurs tiers AWS et en ajustant vos paramètres de recherche jusqu'à ce que vous trouviez la correspondance exacte que vous recherchez.

Lorsque vous recherchez des instances réservées à acheter, vous recevez un devis avec le coût des offres renvoyées. Lorsque vous procédez à l'achat, place AWS automatiquement un prix limite sur le prix d'achat. Le coût total de vos instances réservées ne dépasse pas le montant du devis.

Si le tarif augmente ou change pour quelque raison que ce soit, l'achat n'est pas validé. Lorsque vous achetez l'instance réservée d'un vendeur tiers sur le Marketplace des instances réservées EC2, s'il existe des offres similaires à votre choix mais à un prix initial inférieur, il vous AWS vend les offres au prix initial le plus bas.

Avant de valider votre achat, vérifiez les détails des Instance réservées que vous avez l'intention d'acheter et veillez à ce que tous les paramètres soient exacts. Après avoir acheté une instance réservée (soit auprès d'un vendeur tiers sur le Reserved Instance Marketplace, soit auprès de AWS), vous ne pouvez pas annuler votre achat.

Pour acheter et modifier des instances réservées, assurez-vous que votre utilisateur dispose des autorisations appropriées, telles que la possibilité de décrire les zones de disponibilité. Pour plus d'informations, consultez [the section called "Utiliser instances réservées"](#) (API) ou [the section called "Utiliser instances réservées"](#) (console).

Rubriques

- [Sélection d'une plateforme](#)
- [Mettre votre achat en file d'attente](#)
- [Acheter une instances réservées Standard](#)
- [Acheter instances réservées convertibles](#)
- [Acheter sur le Marketplace Instance réservée](#)
- [Afficher votre instances réservées](#)
- [Annuler un achat mis en file d'attente](#)
- [Renouveler un Instance réservée](#)

Sélection d'une plateforme

Amazon EC2 prend en charge les plateformes suivantes pour les instances réservées :

- Linux/Unix
- Linux avec SQL Server Standard
- Linux avec SQL Server Web
- Linux avec SQL Server Enterprise
- SUSE Linux
- Utilisation de Red Hat Enterprise Linux

- Red Hat Enterprise Linux avec HA
- Windows
- Windows avec SQL Server Standard
- Windows avec SQL Server Web
- Windows avec SQL Server Enterprise

Lorsque vous achetez une Instance réservée, vous devez choisir une offre pour une plateforme qui correspond au système d'exploitation de votre instance.

Instances Linux

- Pour les distributions SUSE Linux et RHEL, vous devez choisir les offres correspondant à ces plateformes spécifiques, c'est-à-dire pour les plateformes SUSE Linux ou Red Hat Enterprise Linux.
- Pour toutes les autres distributions Linux (y compris Ubuntu), choisissez une offre pour la plateforme Linux/UNIX.
- Si vous apportez votre abonnement RHEL existant, vous devez choisir une offre pour la plateforme Linux/UNIX et non une offre pour la plateforme Red Hat Enterprise Linux.

instances Windows

- Pour Windows avec SQL Standard, Windows avec SQL Server Enterprise et Windows avec SQL Server Web, vous devez choisir les offres correspondant à ces plateformes spécifiques.
- Pour toutes les autres versions Windows, choisissez une offre pour la plateforme Windows.

Note

Ubuntu Pro n'est pas disponible en tant qu'instance réservée. Pour réaliser des économies importantes par rapport à la tarification des instances à la demande, nous vous recommandons d'utiliser Ubuntu Pro avec Savings Plans. Pour plus d'informations, consultez le [Guide de l'utilisateur des Savings Plans](#).

Important

Si vous prévoyez d'acheter une instance réservée à appliquer à une instance à la demande qui a été lancée à partir d'une AMI AWS Marketplace, vérifiez d'abord le champ `PlatformDetails` de l'AMI. Le champ `PlatformDetails` indique quelle Instance réservée acheter. Les détails de la plate-forme de l'AMI doivent correspondre à la plate-forme de l'Instance réservée, sinon l'Instance réservée ne sera pas appliquée à l'instance à la demande. Pour plus d'informations sur la façon d'afficher les détails de la plate-forme de l'AMI, reportez-vous à la section [Comprendre les informations de facturation d'AMI](#).

Mettre votre achat en file d'attente

Par défaut, lorsque vous achetez une Instance réservée, l'achat est effectué immédiatement. Vous pouvez également mettre vos achats en file d'attente pour une date et une heure futures. Par exemple, vous pouvez mettre un achat en file d'attente jusqu'à ce qu'une Instance réservée existante expire. Cela peut vous aider à garantir une couverture ininterrompue.

Vous pouvez mettre en file d'attente des achats pour une instances réservées régionale, mais pas pour une instances réservées de zone ou une instances réservées d'autres vendeurs. Vous pouvez mettre un achat en file d'attente jusqu'à trois ans en avance. À l'heure et la date prévues, l'achat est effectué à l'aide du mode de paiement par défaut. Une fois le paiement réussi, l'avantage de facturation est appliqué.

Vous pouvez afficher vos achats mis en file d'attente dans la console Amazon EC2. Le statut d'un achat mis en file d'attente est `queued`. Vous pouvez annuler un achat mis en file d'attente à tout moment avant son heure planifiée. Pour plus de détails, consultez [Annuler un achat mis en file d'attente](#).

Acheter une instances réservées Standard

Vous pouvez acheter des instances réservées standard dans une zone de disponibilité spécifique et obtenir une réservation de capacité. Vous avez également la possibilité de renoncer à la réservation de capacité et d'acheter une Instance réservée standard régionale.

New console

Pour acheter des instances réservées standard à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, choisissez Instances réservées, puis Acheter des Instances réservées.
3. Pour Offering class (Classe d'offre), sélectionnez Standard pour afficher les Instances réservées standard.
4. Pour acheter une réservation de capacité, basculez sur Only show offerings that reserve capacity (Ne montre que les offres réservant une capacité) dans le coin supérieur droit de l'écran d'achat. Lorsque vous basculez sur ce paramètre, le champ Availability Zone (Zone de disponibilité) apparaît.

Pour acheter une Instance réservée régionale, désactivez ce paramètre. Lorsque vous désactivez ce paramètre, le champ Availability Zone (Zone de disponibilité) disparaît.

5. Sélectionnez d'autres configurations en fonction de vos besoins, puis sélectionnez Search (Recherche).
6. Pour chaque Instance réservée que vous souhaitez acheter, saisissez la quantité désirée et sélectionnez Add to cart (Ajouter au panier).

Pour acheter une instance réservée standard sur la marketplace des instances réservées, recherchez 3rd party (Tiers) dans la colonne Seller (Vendeur) des résultats de recherche. La colonne Durée affiche des durées non standard. Pour plus d'informations, consultez [Acheter sur le Marketplace Instance réservée](#).

7. Pour afficher un récapitulatif des Instances réservées sélectionnées, sélectionnez View cart (Afficher le panier).
8. Si Order On (Commander le) correspond à Now (Maintenant), l'achat est terminé après que vous avez sélectionné Order all (Commander tout). Pour mettre un achat en file d'attente, choisissez Maintenant et sélectionnez une date. Vous pouvez sélectionner une date différente pour chaque offre éligible dans le panier. L'achat est mis en file d'attente jusqu'à minuit UTC à la date sélectionnée.
9. Pour valider la commande, sélectionnez Order all (Commander tout).

Si, au moment de passer la commande, il existe des offres similaires à votre choix mais à un prix inférieur, vous AWS vend les offres au prix inférieur.

10. Choisissez Fermer.

L'état de votre commande figure dans la colonne État. Une fois votre commande terminée, la valeur État passe de Payment-pending à Active. Lorsque l'Instance réservée est Active, elle est prête à être utilisée.

 Note

Si le statut passe à `Retired`, votre paiement n'a AWS peut-être pas été reçu.

Old console

Pour acheter des instances réservées standard à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances réservées, puis Acheter des Instances réservées.
3. Pour Offering class (Classe d'offre), sélectionnez Standard pour afficher les Instances réservées standard.
4. Pour acheter une réservation de capacité, choisissez Ne montre que les offres réservant une capacité dans le coin supérieur droit de l'écran d'achat. Pour acheter une Instance réservée régionale, laissez la case à cocher désactivée.
5. Sélectionnez d'autres configurations en fonction de vos besoins, puis choisissez Recherche.

Pour acheter une instance réservée standard sur la marketplace des instances réservées, recherchez 3rd Party (Tiers) dans la colonne Seller (Vendeur) des résultats de recherche. La colonne Durée affiche des durées non standard.

6. Pour chaque Instance réservée que vous souhaitez acheter, saisissez la quantité et sélectionnez Add to Cart (Ajouter au panier).
7. Pour afficher un récapitulatif des Instances réservées sélectionnées, sélectionnez View cart (Afficher le panier).
8. Si Order On (Commander le) est Maintenant, l'achat est terminé immédiatement. Pour mettre un achat en file d'attente, choisissez Maintenant et sélectionnez une date. Vous pouvez sélectionner une date différente pour chaque offre éligible dans le panier. L'achat est mis en file d'attente jusqu'à minuit UTC à la date sélectionnée.
9. Pour valider la commande, choisissez Order (Commander).

Si, au moment de passer la commande, il existe des offres similaires à votre choix mais à un prix inférieur, vous AWS vend les offres au prix inférieur.

10. Choisissez Fermer.

L'état de votre commande figure dans la colonne État. Une fois votre commande terminée, la valeur État passe de `payment-pending` à `active`. Lorsque l'Instance réservée est active, elle est prête à être utilisée.

 Note

Si le statut passe à `retired`, votre paiement n'a AWS peut-être pas été reçu.

Pour acheter une instance réservée standard à l'aide du AWS CLI

1. Pour rechercher les Instances réservées disponibles, utilisez la commande [describe-reserved-instances-offerings](#). Spécifiez `standard` pour le paramètre `--offering-class` afin de renvoyer uniquement des Instances réservées standard. Vous pouvez appliquer des paramètres supplémentaires pour affiner vos résultats. Par exemple, si vous souhaitez acheter une Instance réservée `t2.large` régionale avec une location par défaut pour Linux/UNIX pour une durée d'un an seulement :

```
aws ec2 describe-reserved-instances-offerings \  
  --instance-type t2.large \  
  --offering-class standard \  
  --product-description "Linux/UNIX" \  
  --instance-tenancy default \  
  --filters Name=duration,Values=31536000 Name=scope,Values=Region
```

Pour rechercher des instances réservées sur la marketplace des instances réservées uniquement, utilisez le filtre `marketplace` et ne spécifiez pas de durée dans la demande, puisque la durée peut être inférieure à 1 ou 3 ans.

```
aws ec2 describe-reserved-instances-offerings \  
  --instance-type t2.large \  
  --offering-class standard \  
  --product-description "Linux/UNIX" \  
  --instance-tenancy default \  
  --filters Name=marketplace,Values=true
```

Lorsque vous trouvez une Instance réservée qui correspond à vos besoins, notez l'ID de l'offre.

Exemples :

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Utilisez la commande [purchase-reserved-instances-offering](#) pour acheter une Instance réservée. Vous devez spécifier l'ID d'offre d'Instance réservée que vous avez obtenu à l'étape précédente et indiquer le nombre d'instances pour la réservation.

```
aws ec2 purchase-reserved-instances-offering \  
  --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \  
  --instance-count 1
```

Par défaut, l'achat est terminé immédiatement. Pour mettre l'achat en file d'attente, vous pouvez également ajouter le paramètre suivant à l'appel précédent.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Utilisez la commande [describe-reserved-instances](#) pour obtenir le statut de votre Instance réservée.

```
aws ec2 describe-reserved-instances
```

Vous pouvez également utiliser les AWS Tools for Windows PowerShell commandes suivantes :

- [Get-EC2ReservedInstancesOffering](#)
- [New-EC2ReservedInstance](#)
- [Get-EC2ReservedInstance](#)

Une fois l'achat terminé, si vous avez déjà une instance en cours d'exécution qui correspond aux attributs de l'Instance réservée, l'avantage de facturation est immédiatement appliqué. Vous n'avez pas besoin de redémarrer vos instances. Si vous n'avez pas d'instance en cours d'exécution adéquate, lancez une instance et veillez à respecter les mêmes critères que ceux spécifiés pour l'Instance réservée. Pour plus d'informations, consultez [Utiliser votre instances réservées](#).

Pour des exemples de la façon dont les Instances réservées sont appliquées à vos instances en cours d'exécution, consultez [Application des instances réservées](#).

Acheter instances réservées convertibles

Vous pouvez acheter des instances réservées convertibles dans une zone de disponibilité spécifique et obtenir une réservation de capacité. Vous avez également la possibilité de renoncer à la réservation de capacité et d'acheter une Instance réservée convertible régionale.

New console

Pour acheter des instances réservées convertibles à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances réservées, puis Acheter des Instances réservées.
3. Pour Offering class (Classe d'offre), sélectionnez Convertible pour afficher des Instances réservées convertibles.
4. Pour acheter une réservation de capacité, basculez sur Only show offerings that reserve capacity (Ne montre que les offres réservant une capacité) dans le coin supérieur droit de l'écran d'achat. Lorsque vous basculez sur ce paramètre, le champ Availability Zone (Zone de disponibilité) apparaît.

Pour acheter une Instance réservée régionale, désactivez ce paramètre. Lorsque vous désactivez ce paramètre, le champ Availability Zone (Zone de disponibilité) disparaît.

5. Sélectionnez d'autres configurations en fonction de vos besoins, puis choisissez Recherche.
6. Pour chaque Instance réservée convertible que vous souhaitez acheter, saisissez la quantité et sélectionnez Add to cart (Ajouter au panier).
7. Pour afficher un résumé de votre sélection, sélectionnez View cart (Afficher le panier).
8. Si Order On (Commander le) correspond à Now (Maintenant), l'achat est terminé après que vous avez sélectionné Order all (Commander tout). Pour mettre un achat en file d'attente, choisissez Maintenant et sélectionnez une date. Vous pouvez sélectionner une date différente pour chaque offre éligible dans le panier. L'achat est mis en file d'attente jusqu'à minuit UTC à la date sélectionnée.
9. Pour valider la commande, sélectionnez Order all (Commander tout).

Si, au moment de passer la commande, il existe des offres similaires à votre choix mais à un prix inférieur, vous AWS vend les offres au prix inférieur.

10. Choisissez Fermer.

L'état de votre commande figure dans la colonne État. Une fois votre commande terminée, la valeur État passe de Payment-pending à Active. Lorsque l'Instance réservée est Active, elle est prête à être utilisée.

 Note

Si le statut passe à Retired, votre paiement n'a AWS peut-être pas été reçu.

Old console

Pour acheter des instances réservées convertibles à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances réservées, puis Acheter des Instances réservées.
3. Pour Offering class (Classe d'offre), sélectionnez Convertible pour afficher des Instances réservées convertibles.
4. Pour acheter une réservation de capacité, choisissez Ne montre que les offres réservant une capacité dans le coin supérieur droit de l'écran d'achat. Pour acheter une Instance réservée régionale, laissez la case à cocher désactivée.
5. Sélectionnez d'autres configurations en fonction de vos besoins, puis choisissez Recherche.
6. Pour chaque Instance réservée convertible que vous souhaitez acheter, saisissez la quantité et sélectionnez Add to Cart (Ajouter au panier).
7. Pour afficher un résumé de votre sélection, sélectionnez View cart (Afficher le panier).
8. Si Order On (Commander le) est Maintenant, l'achat est terminé immédiatement. Pour mettre un achat en file d'attente, choisissez Maintenant et sélectionnez une date. Vous pouvez sélectionner une date différente pour chaque offre éligible dans le panier. L'achat est mis en file d'attente jusqu'à minuit UTC à la date sélectionnée.
9. Pour valider la commande, choisissez Order (Commander).

Si, au moment de passer la commande, il existe des offres similaires à votre choix mais à un prix inférieur, vous AWS vend les offres au prix inférieur.

10. Choisissez Fermer.

L'état de votre commande figure dans la colonne État. Une fois votre commande terminée, la valeur État passe de `payment-pending` à `active`. Lorsque l'Instance réservée est active, elle est prête à être utilisée.

 Note

Si le statut passe à `retired`, votre paiement n'a AWS peut-être pas été reçu.

Pour acheter une instance réservée convertible à l'aide du AWS CLI

1. Pour rechercher les Instances réservées disponibles, utilisez la commande [describe-reserved-instances-offerings](#). Spécifiez `convertible` pour le paramètre `--offering-class` afin de renvoyer uniquement des Instances réservées convertibles. Vous pouvez appliquer des paramètres supplémentaires pour affiner vos résultats. Par exemple, si vous voulez acheter une Instance réservée `t2.large` régionale à location par défaut pour Linux/UNIX :

```
aws ec2 describe-reserved-instances-offerings \  
  --instance-type t2.large \  
  --offering-class convertible \  
  --product-description "Linux/UNIX" \  
  --instance-tenancy default \  
  --filters Name=scope,Values=Region
```

Lorsque vous trouvez une Instance réservée qui correspond à vos besoins, notez l'ID de l'offre. Exemples :

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Utilisez la commande [purchase-reserved-instances-offering](#) pour acheter une Instance réservée. Vous devez spécifier l'ID d'offre d'Instance réservée que vous avez obtenu à l'étape précédente et indiquer le nombre d'instances pour la réservation.

```
aws ec2 purchase-reserved-instances-offering \  
  --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \  
  --instance-count 1
```

Par défaut, l'achat est terminé immédiatement. Pour mettre l'achat en file d'attente, vous pouvez également ajouter le paramètre suivant à l'appel précédent.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Utilisez la commande [describe-reserved-instances](#) pour obtenir le statut de votre Instance réservée.

```
aws ec2 describe-reserved-instances
```

Vous pouvez également utiliser les AWS Tools for Windows PowerShell commandes suivantes :

- [Get-EC2ReservedInstancesOffering](#)
- [New-EC2ReservedInstance](#)
- [Get-EC2ReservedInstance](#)

Si vous avez déjà une instance en cours d'exécution qui correspond aux attributs de l'Instance réservée, l'avantage de facturation est immédiatement appliqué. Vous n'avez pas besoin de redémarrer vos instances. Si vous n'avez pas d'instance en cours d'exécution adéquate, lancez une instance et veillez à respecter les mêmes critères que ceux spécifiés pour l'Instance réservée. Pour plus d'informations, consultez [Utiliser votre instances réservées](#).

Pour des exemples de la façon dont les Instances réservées sont appliquées à vos instances en cours d'exécution, consultez [Application des instances réservées](#).

Acheter sur le Marketplace Instance réservée

Vous pouvez acheter des instances réservées auprès de vendeurs tiers qui possèdent des instances réservées dont ils n'ont plus besoin sur la marketplace des instances réservées. Vous pouvez effectuer cette opération à l'aide de la console Amazon EC2 ou d'un outil de ligne de commande. Le processus est similaire à l'achat d'instances réservées auprès de AWS. Pour plus d'informations, consultez [Acheter une instances réservées Standard](#).

Il existe quelques différences entre les instances réservées achetées sur le Reserved Instance Marketplace et les instances réservées achetées directement auprès de AWS :

- **Durée** – Les instances réservées que vous achetez auprès de tiers ont une durée inférieure à la durée standard complète. Conditions générales complètes à compter d' AWS une durée d'un an ou de trois ans.
- **Prix initial** – Les instances réservées tierces peuvent être vendues à différents prix initiaux. Les frais d'utilisation ou récurrents restent les mêmes que ceux fixés lors de l'achat initial des instances réservées AWS.
- **Types d'instances réservées** – Seules les instances réservées standard Amazon EC2 peuvent être achetées sur la marketplace des instances réservées. Les instances réservées convertibles, Amazon RDS et Amazon ElastiCache Reserved Instances ne sont pas disponibles à l'achat sur le Reserved Instance Marketplace.

Les informations principales vous concernant sont communiquées au vendeur, par exemple votre code postal et votre pays de résidence.

Ces informations permettent au vendeur de calculer toutes les taxes destinées au gouvernement qui sont susceptibles d'être appliquées aux transactions (par exemple, les taxes de vente ou la TVA). Elles sont communiquées sous la forme d'un rapport de décaissement. Dans de rares cas, vous devrez AWS peut-être fournir votre adresse e-mail au vendeur afin qu'il puisse vous contacter pour toute question relative à la vente (par exemple, des questions fiscales).

Pour des raisons similaires, AWS partage le nom de l'entité juridique du vendeur sur la facture d'achat de l'acheteur. Si vous avez besoin d'informations supplémentaires sur le vendeur pour des raisons fiscales ou autres, contactez [AWS Support](#).

Afficher vos instances réservées

Vous pouvez afficher les instances réservées que vous avez achetées à l'aide de la console Amazon EC2 ou d'un outil de ligne de commande.

Pour afficher vos instances réservées sur la console

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Vos instances réservées mises en file d'attente, actives et mises hors service sont répertoriées. La colonne État indique l'état.
4. Si vous êtes vendeur sur la marketplace des instances réservées, l'onglet My Listings (Mes listes) indique le statut d'une réservation répertoriée sur la [marketplace des instances réservées](#). Pour plus d'informations, consultez [États de la liste des éléments Instance réservée](#).

Pour afficher vos instances réservées à l'aide de la ligne de commande

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#)(Outils pour Windows PowerShell)

Annuler un achat mis en file d'attente

Vous pouvez mettre un achat en file d'attente jusqu'à trois ans en avance. Vous pouvez annuler un achat mis en file d'attente à tout moment avant son heure planifiée.

New console

Pour annuler un achat mis en file d'attente

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Sélectionnez une ou plusieurs instances réservées.
4. Sélectionnez Actions, Delete queued Reserved Instances (Supprimer les instances réservées mises en file d'attente).
5. Lorsque vous êtes invité à confirmer, sélectionnez Delete (Supprimer), puis sélectionnez Close (Fermer).

Old console

Pour annuler un achat mis en file d'attente

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Sélectionnez une ou plusieurs instances réservées.
4. Sélectionnez Actions, Delete Queued Reserved Instance (Supprimer les instances réservées mises en file d'attente).
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Yes, Delete.

Pour annuler un achat en file d'attente à l'aide de la ligne de commande

- [delete-queued-reserved-instances](#) (AWS CLI)

- [Remove-EC2QueuedReservedInstance](#)(Outils pour Windows PowerShell)

Renouveler un Instance réservée

Vous pouvez renouveler une Instance réservée avant qu'elle n'entre en phase d'expiration. Le renouvellement d'une Instance réservée met en file d'attente l'achat d'une Instance réservée possédant la même configuration jusqu'à ce que l'Instance réservée actuelle expire.

New console

Pour renouveler une instance réservée à l'aide d'un achat en file d'attente

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Reserved Instances (Instances réservées).
3. Sélectionnez l'instance réservée à renouveler.
4. Choisissez Actions, Renew Reserved Instances (Renouveler les instances réservées).
5. Pour valider la commande, sélectionnez Order all (Commander tout), puis Close (Fermer).

Old console

Pour renouveler une instance réservée à l'aide d'un achat en file d'attente

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Reserved Instances (Instances réservées).
3. Sélectionnez l'instance réservée à renouveler.
4. Choisissez Actions, Renew Reserved Instances (Renouveler les instances réservées).
5. Pour valider la commande, choisissez Order (Commander).

Vendre sur la marketplace des instances réservées

La Reserved Instance Marketplace est une plateforme qui prend en charge la vente d'instances réservées standard non utilisées par des tiers et des AWS clients, dont la durée et les options tarifaires varient. Par exemple, vous souhaitez peut-être vendre des instances réservées après avoir déplacé des instances vers une nouvelle AWS région, changé de type d'instance, mis fin à des projets avant l'expiration du terme, lorsque les besoins de votre entreprise évoluent ou si vous disposez de capacités inutiles.

Dès que vous listez vos instances réservées sur la marketplace des instances réservées, elles deviennent disponibles et des acheteurs potentiels peuvent se les procurer. Toutes les instances réservées sont regroupées selon la durée de réservation restante et le taux horaire.

Pour répondre à la demande d'un acheteur d'acheter l'instance réservée d'un vendeur tiers via le Marketplace des instances réservées EC2, vendez d' AWS abord l'instance réservée au prix initial le plus bas du groupe spécifié. AWS Vend ensuite l'instance réservée au prix le plus bas suivant, jusqu'à ce que la totalité de la commande de l'acheteur soit exécutée. AWS traite ensuite les transactions et transfère la propriété des instances réservées à l'acheteur.

Vous êtes le propriétaire de l'Instance réservée jusqu'à ce qu'elle soit vendue. Une fois la vente conclue, vous ne disposez plus de la réservation de capacité et vous n'êtes plus soumis aux frais récurrents avec remise. Si vous continuez à utiliser votre instance, le prix à la demande vous sera AWS facturé à compter du moment où votre instance réservée a été vendue.

Si vous voulez vendre vos instances réservées inutilisées sur la marketplace des instances réservées, vous devez respecter certains critères d'éligibilité.

Pour plus d'informations sur l'achat d'instances réservées sur la marketplace des instances réservées, consultez [Acheter sur le Marketplace Instance réservée](#).

Sommaire

- [Limites et restrictions](#)
- [S'inscrire en tant que vendeur](#)
- [Compte bancaire pour les décaissements](#)
- [Informations fiscales](#)
- [Définir le prix de votre instances réservées](#)
- [Lister votre instances réservées](#)
- [États de la liste des éléments Instance réservée](#)
- [Cycle de vie d'une liste](#)
- [Après la vente de votre Instance réservée](#)
- [Obtention du paiement](#)
- [Communication des informations à l'acheteur](#)

Limites et restrictions

Avant de pouvoir vendre vos réservations inutilisées, vous devez vous inscrire en tant que vendeur sur la marketplace des instances réservées. Pour plus d'informations, consultez [S'inscrire en tant que vendeur](#).

Les restrictions et restrictions suivantes s'appliquent à la vente d'instances réservées :

- Seules les instances réservées régionales et zonales standard Amazon EC2 peuvent être vendues sur la marketplace des instances réservées.
- Les instances réservées convertibles Amazon EC2 ne peuvent pas être vendues sur la marketplace des instances réservées.
- Les instances réservées pour d'autres AWS services, tels qu'Amazon RDS et Amazon ElastiCache, ne peuvent pas être vendues sur le Reserved Instance Marketplace.
- L'Instance réservée standard doit être valable pendant encore au moins un mois.
- Vous ne pouvez pas vendre une Instance réservée standard dans une région [désactivée par défaut](#).
- Le tarif minimum autorisé sur la marketplace des instances réservées est de 0,00 USD.
- Vous pouvez vendre des instances réservées sans frais initiaux, avec frais initiaux partiels ou au paiement total anticipé sur le Marketplace des instances réservées, à condition qu'elles soient actives sur votre compte depuis au moins 30 jours. En outre, s'il y a un paiement initial sur une instance réservée, elle ne peut être vendue qu'après la réception par AWS du paiement initial.
- Vous ne pouvez pas modifier directement votre liste sur la marketplace des instances réservées. Toutefois, vous pouvez la changer en commençant par l'annuler, puis en créant une autre liste avec de nouveaux paramètres. Pour plus d'informations, consultez [Définir le prix de votre instances réservées](#). Vous pouvez également modifier vos instances réservées avant de les inclure dans votre liste. Pour plus d'informations, consultez [Modifier instances réservées](#).
- AWS facture des frais de service de 12 % du prix initial total de chaque instance réservée standard que vous vendez sur le Reserved Instance Marketplace. Le prix initial correspond au prix demandé par le vendeur pour l'Instance réservée standard.
- Lorsque vous vous inscrivez en tant que vendeur, la banque que vous spécifiez doit avoir une adresse aux États-Unis. Pour plus d'informations, consultez [Exigences supplémentaires du vendeur pour les produits payés](#) dans le Guide du vendeur AWS Marketplace .
- Les clients d'Amazon Web Services India Private Limited (AWS Inde) ne peuvent pas vendre d'instances réservées sur le Reserved Instance Marketplace, même s'ils possèdent un compte

bancaire américain. Pour plus d'informations, voir [Quelles sont les différences entre les comptes AWS indiens Comptes AWS et les comptes indiens ?](#)

S'inscrire en tant que vendeur

 Note

Ils sont les seuls à Utilisateur racine d'un compte AWS pouvoir créer un compte en tant que vendeur.

Pour vendre sur la marketplace des instances réservées, vous devez tout d'abord vous inscrire comme vendeur. Lors de l'enregistrement, vous devez fournir les informations suivantes lors de l'enregistrement :

- Informations bancaires : vous AWS devez disposer de vos informations bancaires afin de décaisser les fonds collectés lorsque vous vendez vos réservations. La banque que vous spécifiez doit avoir une adresse aux États-Unis. Pour plus d'informations, consultez [Compte bancaire pour les décaissements](#).
- Questionnaire fiscal : tous les vendeurs doivent répondre à un questionnaire fiscal afin de déterminer les obligations de déclaration fiscale éventuelles. Pour plus d'informations, consultez [Informations fiscales](#).

Après avoir AWS reçu votre inscription de vendeur terminée, vous recevez un e-mail confirmant votre inscription et vous informant que vous pouvez commencer à vendre sur le Reserved Instance Marketplace.

Compte bancaire pour les décaissements

AWS devez disposer de vos informations bancaires afin de déboursier les fonds collectés lorsque vous vendez votre instance réservée. La banque que vous spécifiez doit avoir une adresse aux États-Unis. Pour plus d'informations, consultez [Exigences supplémentaires du vendeur pour les produits payés](#) dans le Guide du vendeur AWS Marketplace .

Pour enregistrer un compte par défaut destiné aux décaissements

1. Ouvrez la page [Reserved Instance Marketplace Seller Registration](#) (Inscription vendeur sur la marketplace des instances réservées) et connectez-vous à l'aide de vos informations d'identification AWS .
2. Sur la page Manage Bank Account (Gérer le compte bancaire), entrez les informations suivantes concernant la banque qui recevra vos paiements :
 - Nom du titulaire du compte bancaire
 - Code d'acheminement
 - Numéro de compte
 - Type de compte bancaire

Note

Si vous utilisez le compte bancaire de votre société, vous êtes invité à envoyer les informations relatives au compte bancaire par télécopie au 1-206-765-3424.

Une fois l'enregistrement terminé, le compte bancaire spécifié est utilisé par défaut, dans l'attente d'une vérification auprès de la banque. Cette opération peut prendre jusqu'à deux semaines, une période au cours de laquelle vous ne pouvez pas recevoir de décaissements. Pour un compte établi, deux jours sont généralement nécessaires à l'exécution d'un décaissement.

Pour modifier le compte bancaire par défaut utilisé pour les décaissements

1. Sur la page [Reserved Instance Marketplace Seller Registration](#) (Inscription vendeur sur la marketplace des instances réservées), connectez-vous avec le compte utilisé pour l'inscription.
2. Sur la page Manage Bank Account (Gérer le compte bancaire), ajoutez un nouveau compte bancaire ou modifiez le compte défini par défaut.

Informations fiscales

Votre vente d'instances réservées peut être soumise à une taxe appliquée aux transactions, telle qu'une taxe de vente ou une TVA. Vérifiez auprès du service fiscal, juridique, financier ou comptable de votre entreprise afin de déterminer si des taxes sont applicables aux transactions concernées.

Il vous incombe de collecter et d'envoyer les taxes applicables aux transactions à l'administration fiscale appropriée.

Dans le cadre du processus d'enregistrement du vendeur, vous devez remplir un questionnaire d'ordre fiscal dans le [Seller Registration Portal](#). Le questionnaire collecte vos informations fiscales et remplit un formulaire IRS W-9, W-8BEN ou W-8BEN-E, utilisé pour déterminer les éventuelles obligations de déclaration fiscale.

Les informations fiscales que vous renseignez dans le questionnaire peuvent différer selon que vous œuvrez comme personne morale ou physique, et que votre entreprise est une entité ou personne américaine ou non. En remplissant ce questionnaire, gardez les points suivants à l'esprit :

- Les informations fournies par AWS, y compris les informations contenues dans cette rubrique, ne constituent pas des conseils fiscaux, juridiques ou autres conseils professionnels. Pour découvrir en quoi les obligations de déclaration imposées par l'IRS affectent votre entreprise, ou pour toute autre question, contactez votre conseiller fiscal, juridique ou autre.
- Pour vous conformer aux exigences de l'IRS en matière de déclarations aussi efficacement que possible, répondez à toutes les questions et entrez toutes les informations demandées au cours du questionnaire.
- Vérifiez vos réponses. Évitez les fautes de frappe ou la saisie de numéros d'identification fiscale inexacts. Ces erreurs risqueraient d'entraîner le refus de votre formulaire fiscal.

Selon vos réponses au questionnaire et les seuils de déclaration de l'IRS, Amazon peut soumettre le formulaire 1099-K. Vous en recevrez une copie par voie postale au plus tard le 31 janvier de l'année suivant celle où votre compte fiscal a atteint les niveaux de seuil. Par exemple, si votre compte fiscal atteint le seuil en 2018, vous recevrez le formulaire 1099-K le 31 janvier 2019 au plus tard.

Pour en savoir plus sur les exigences de l'IRS et sur le formulaire 1099-K, consultez le site web de l'[IRS](#).

Définir le prix de votre instances réservées

Tenez compte des éléments suivants lorsque vous fixez le prix de vos instances réservées :

- Prix initial – Le prix initial est le seul prix que vous puissiez spécifier pour l'instance réservée que vous vendez. Le prix initial est le prix unique que l'acheteur paie lorsqu'il achète une instance réservée.

Étant donné que la valeur des instances réservées diminue au fil du temps, AWS vous pouvez par défaut définir les prix pour qu'ils diminuent par tranches égales d'un mois à l'autre. Toutefois, vous pouvez définir des tarifs initiaux différents en fonction du moment de vente de votre réservation. Par exemple, si votre Instance réservée est encore valide pendant neuf mois, vous pouvez indiquer le montant que vous accepteriez si un client achetait cette Instance réservée au cours des neuf mois restants. Vous pouvez définir un autre prix avec cinq mois restants, et encore un autre avec un mois restant.

Le tarif minimum autorisé sur la marketplace des instances réservées est de 0,00 USD.

- Limites – Les limites suivantes relatives pour la vente d'instances réservées s'appliquent à la durée de vie de votre Compte AWS. Il ne s'agit pas de limites annuelles.
 - Vous pouvez vendre jusqu'à 50 000 USD d'Instances réservées.
 - Vous pouvez vendre jusqu'à 5 000 Instances réservées.

Ces limites ne peuvent généralement pas être augmentées, mais elles seront case-by-case évaluées sur demande. Pour demander une augmentation des limites, remplissez le formulaire de demande d'[augmentation de limite de service](#). Pour Type de limite, choisissez Ventes d'instances réservées EC2.

- Ne peut pas modifier – Vous ne pouvez pas modifier votre liste directement. Toutefois, vous pouvez la changer en commençant par l'annuler, puis en créant une autre liste avec de nouveaux paramètres.
- Peut annuler – Vous pouvez annuler votre liste à tout moment, tant qu'elle est dans l'état active. Vous ne pouvez pas annuler une liste si elle fait déjà l'objet d'une correspondance ou si sa vente est en cours de traitement. Si certaines instances de votre liste font l'objet d'une correspondance et que vous annulez la liste, seules les instances restantes qui ne font pas l'objet d'une correspondance sont supprimées de la liste.

Lister votre instances réservées

En tant que vendeur enregistré, vous pouvez choisir de vendre une ou plusieurs de vos instances réservées. Vous pouvez choisir de les vendre toutes sur une même liste ou par sections. En outre, vous pouvez ajouter à la liste les instances réservées avec n'importe quelle configuration de type d'instance, plateforme et portée.

La console détermine une suggestion de prix. Elle vérifie les offres qui correspondent à votre Instance réservée et sélectionne celle dont le prix est le plus bas. Sinon, elle calcule un prix suggéré

basé sur le coût de l'Instance réservée pour le temps restant. Si la valeur calculée est inférieure à 1,01 USD, le prix suggéré est de 1,01 USD.

Si vous annulez votre liste et qu'une partie de celle-ci a déjà été vendue, l'annulation ne s'applique pas à la partie déjà vendue. Seule la partie de la liste non encore vendue n'est plus disponible sur la marketplace des instances réservées.

Pour répertorier une instance réservée sur le Reserved Instance Marketplace à l'aide du AWS Management Console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Sélectionnez les Instances réservées à répertorier, puis choisissez Actions, Vendre des Instances réservées.
4. Sur la page Configuration de votre liste d'Instance réservée définissez le nombre d'instances à vendre et le prix initial pour la durée restante dans les colonnes appropriées. Pour afficher l'évolution de la valeur de votre réservation au cours de la durée restante, sélectionnez la flèche en regard de la colonne Mois restant.
5. Si vous êtes un utilisateur avancé et que vous souhaitez personnaliser la tarification, vous pouvez entrer différentes valeurs pour les mois suivants. Pour revenir à la baisse de prix linéaire par défaut, choisissez Réinitialiser.
6. Choisissez Continuer une fois la configuration de la liste terminée.
7. Vérifiez les détails de votre liste sur la page Configuration de votre liste d'Instance réservée. Si vous n'avez rien à modifier, choisissez Répertorier l'instance réservée.

Pour afficher vos listes sur la console

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Sélectionnez l'Instance réservée que vous avez répertoriée et choisissez l'onglet Mes listes en bas de la page.

Pour gérer les instances réservées sur le Reserved Instance Marketplace à l'aide du AWS CLI

1. Obtenez la liste de vos Instances réservées en utilisant la commande [describe-reserved-instances](#).

2. Notez l'ID de l'Instance réservée que vous souhaitez répertorier et appelez [create-reserved-instances-listing](#). Vous devez spécifier l'ID de l'Instance réservée, le nombre d'instances et le barème de tarification.
3. Pour afficher votre liste, utilisez la commande [describe-reserved-instances-listings](#).
4. Pour annuler votre liste, utilisez la commande [cancel-reserved-instances-listings](#).

États de la liste des éléments Instance réservée

État de la liste de l'onglet Mes listes de la page des Instances réservées affiche le statut actuel de vos listes :

Les informations figurant dans Listing State (État de la liste) concernent l'état de votre liste sur la marketplace des instances réservées. Elles diffèrent des informations d'état affichées par la colonne État de la page Instances réservées. Ces informations d'État concernent votre réservation.

- **active** : la liste peut être achetée.
- **canceled (annulée)** : la liste a été annulée et ne peut plus être achetée sur la marketplace des instances réservées.
- **closed (fermée)** : l'Instance réservée figure pas sur la liste. Une Instance réservée peut être `closed` parce que la vente de la liste est terminée.

Cycle de vie d'une liste

Lorsque toutes les instances d'une liste correspondent aux besoins d'un acheteur et sont vendues, l'onglet Mes listes indique que votre Total instance count (Nombre total d'instances) correspond au nombre indiqué sous Vendue. Il n'y a plus aucune instance avec le statut Disponible pour votre liste dont le Statut est désormais `closed`.

Lorsqu'une partie seulement de votre annonce est vendue, AWS les instances réservées sont retirées de l'annonce et crée un nombre d'instances réservées égal au nombre d'instances réservées restant dans le décompte. Par conséquent, l'ID de liste et la liste qu'il représente, et qui a désormais moins de réservations en vente, restent actifs.

Toute vente ultérieure d'instances réservées figurant sur la liste est traitée de cette façon. Lorsque toutes les instances réservées de la liste sont vendues, AWS marque l'offre comme `closed`.

Par exemple, vous créez une liste ID de liste d'instances réservées `5ec28771-05ff-4b9b-aa31-9e57dexample`. Cette liste comporte 5 instances.

L'onglet Mes listes de la page de console Instance réservée affiche la liste de cette façon :

ID de liste d'Instance réservée 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 0
- Available = 5
- Status = active

Un acheteur achète deux de ces réservations, ce qui laisse trois réservations encore disponibles à la vente. En raison de cette vente partielle, AWS crée une réservation avec trois instances correspondant à celles qui peuvent encore être achetées.

Voici comment votre liste apparaît sous l'onglet Mes listes :

ID de liste d'Instance réservée 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 2
- Available = 3
- Status = active

Si vous annulez votre liste et qu'une partie de celle-ci a déjà été vendue, l'annulation ne s'applique pas à la partie déjà vendue. Seule la partie de la liste non encore vendue n'est plus disponible sur la marketplace des instances réservées.

Après la vente de votre Instance réservée

Lorsque votre instance réservée est vendue, vous AWS envoie une notification par e-mail. Vous êtes averti par e-mail de toutes les activités quotidiennes vous concernant. Les activités peuvent inclure la création ou la vente d'une annonce, ou l'AWS envoi de fonds sur votre compte.

Pour suivre le statut d'une liste d'Instance réservée dans la console

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances réservées.
3. Cliquez sur l'onglet Mes listes.

L'onglet Mes listes contient la valeur État de la liste. Il contient aussi des informations sur la durée, le tarif et le nombre d'instances disponibles, en attente, vendues ou annulées.

Vous pouvez également utiliser la commande [describe-reserved-instances-listings](#) avec le filtre approprié pour obtenir des informations sur vos listes.

Obtention du paiement

Dès AWS réception des fonds de la part de l'acheteur, un message est envoyé à l'adresse e-mail du propriétaire enregistré pour l'instance réservée vendue.

AWS envoie un virement bancaire ACH (Automated Clearing House) sur le compte bancaire que vous avez indiqué. En règle générale, ce virement est effectué entre 1 à 3 jours après la vente de l'Instance réservée. Les décaissements se déroulent une fois par jour. Vous recevrez un e-mail avec un rapport de remboursement une fois que les fonds auront été débloqués. N'oubliez pas que vous pourrez recevoir les décaissements uniquement une fois qu' AWS aura reçu la validation de la part de votre banque. Cela peut prendre jusqu'à deux semaines.

L'Instance réservée que vous avez vendue continue à apparaître lorsque vous décrivez vos instances réservées.

Vous recevez un versement en espèces pour vos instances réservées par virement bancaire directement sur votre compte bancaire. AWS facture des frais de service de 12 % du prix initial total de chaque instance réservée que vous vendez sur le Reserved Instance Marketplace.

Communication des informations à l'acheteur

Lorsque vous vendez sur le Reserved Instance AWS Marketplace, indiquez le nom légal de votre entreprise sur la déclaration de l'acheteur conformément à la réglementation américaine. En outre, si l'acheteur appelle AWS Support parce qu'il doit vous contacter pour une facture ou pour toute autre raison liée aux taxes, il AWS peut être amené à fournir votre adresse e-mail à l'acheteur afin qu'il puisse vous contacter directement.

De la même manière, le code postal et le pays de résidence de l'acheteur sont communiqués au vendeur dans le rapport de décaissement. En tant que vendeur, vous aurez parfois besoin de joindre ces informations aux taxes que vous remettez au gouvernement (par exemple, les taxes de vente ou la TVA) pour ces transactions.

AWS ne peut pas fournir de conseils fiscaux, mais si votre fiscaliste détermine que vous avez besoin d'informations supplémentaires spécifiques, [contactez AWS Support](#).

Modifier instances réservées

Lorsque vos besoins évoluent, vous pouvez modifier vos instances réservées standards ou convertibles et continuer à bénéficier de votre avantage de facturation. Vous pouvez modifier des attributs tels que la zone de disponibilité, la taille d'instance (au sein de la même famille et génération d'instances) et la portée de votre instance réservée.

Note

Vous pouvez également échanger une Instance réservée convertible contre une autre Instance réservée convertible avec une configuration différente. Pour plus d'informations, consultez [Échanger des instances réservées convertibles](#).

Vous pouvez modifier toutes vos instances réservées ou un sous-ensemble. Vous pouvez séparer les instances réservées initiales en deux nouvelles instances réservées ou plus. Par exemple, si vous avez une réservation pour 10 instances dans us-east-1a et que vous décidez de déplacer 5 instances vers us-east-1b, la demande de modification entraîne la création de deux réservations : une pour 5 instances dans us-east-1a et l'autre pour 5 instances dans us-east-1b.

Vous pouvez aussi fusionner deux Instances réservées ou plus dans une Instance réservée unique. Par exemple, si vous avez quatre Instances réservées t2.small d'une instance chacune, vous pouvez les fusionner pour créer une Instance réservée t2.large. Pour plus d'informations, consultez [Prise en charge de la modification de tailles d'instances](#).

Après une modification, la tarification des instances réservées est appliquée uniquement aux instances qui correspondent aux nouveaux paramètres. Par exemple, si vous modifiez la zone de disponibilité d'une réservation, les avantages de réservation de capacité et de tarification sont appliqués automatiquement à l'utilisation d'instance dans la nouvelle zone de disponibilité. Les instances qui ne correspondent plus aux nouveaux paramètres sont facturées au taux à la demande à moins que votre compte n'ait d'autres réservations applicables.

Si votre demande de modification a été appliquée :

- La réservation modifiée devient effective immédiatement et l'avantage de tarification est appliqué aux nouvelles instances à partir de l'heure de la demande de modification. Par exemple, si vous avez modifié vos réservations à 21 h 15, l'avantage de tarification est appliqué à votre nouvelle instance à partir de 21 h 00. Vous pouvez obtenir la date d'effet des Instances réservées modifiées en utilisant la commande [describe-reserved-instances](#).

- La réservation initiale est mise hors service. Sa date de fin est la date de début de la nouvelle réservation et la date de fin de la nouvelle réservation est identique à la date de fin de l'Instance réservée initiale. Si vous modifiez une réservation d'une durée de trois ans avec 16 mois restants, la réservation modifiée a une durée de 16 mois, avec la même date de fin que la réservation initiale.
- La réservation modifiée indique un tarif fixe s'élevant à 0 USD et non le tarif fixe de la réservation initiale.
- Le tarif fixe de la réservation modifiée n'a aucune répercussion sur les calculs du niveau tarifaire avec remise appliqué à votre compte. Ces calculs reposent en effet sur le tarif fixe de la réservation initiale.

Si votre demande de modification échoue, vos instances réservées conservent leur configuration d'origine et sont immédiatement disponibles pour une autre demande de modification.

Il n'y a aucun frais pour les modifications et vous ne recevez pas de nouvelles factures.

Vous pouvez modifier vos réservations aussi souvent que vous le souhaitez. Toutefois, vous ne pouvez pas modifier ou annuler une demande de modification en attente une fois que vous l'avez envoyée. Une fois la modification appliquée, vous pouvez envoyer une autre demande de modification afin d'annuler des modifications précédentes, si nécessaire.

Sommaire

- [Conditions obligatoires et restrictions pour toute modification](#)
- [Prise en charge de la modification de tailles d'instances](#)
- [Soumettre des demandes de modification](#)
- [Résoudre les problèmes liés aux demandes de modification](#)

Conditions obligatoires et restrictions pour toute modification

Vous pouvez modifier ces attributs comme suit.

Attribut modifiable	Plateformes prises en charge	Limites et considérations
	Linux et Windows	-

Attribut modifiable	Plateformes prises en charge	Limites et considérations
Changer de zones de disponibilité au sein de la même région		

Attribut modifiable	Plateformes prises en charge	Limites et considérations
Modifier la portée pour passer de Zone de disponibilité à Région et inversement	Linux et Windows	<p>Une instance réservée zonale est étendue à une zone de disponibilité et réserve la capacité dans cette zone de disponibilité. Si vous modifiez la portée de Zone de disponibilité à Région (en d'autres termes, de zonal à régional), vous ne bénéficiez plus de l'avantage de réserve de capacité.</p> <p>Une instance réservée régionale a une portée sur une région. Votre remise d'instance réservée peut s'appliquer aux instances exécutées dans n'importe quelle zone de disponibilité de cette Région. En outre, la remise d'instance réservée s'applique à l'utilisation d'instance de toutes les tailles de la famille d'instances sélectionnée. Si vous modifiez la portée de Région à Zone de disponibilité (en d'autres termes, de régional à zonal), vous perdez la flexibilité de la Zone de disponibilité et la flexibilité de la taille de l'instance (le cas échéant).</p>

Attribut modifiable	Plateformes prises en charge	Limites et considérations
		Pour plus d'informations, consultez Application des instances réservées .
Modification de la taille d'instance au sein de la même famille et génération d'instances	Linux/UNIX uniquement La flexibilité de taille d'instance n'est pas disponible pour les instances réservées sur les autres plateformes, notamment Linux avec SQL Server Standard, Linux avec SQL Server Web, Linux avec SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows avec SQL Standard, Windows avec SQL Server Enterprise et Windows avec SQL Server Web.	La réservation doit utiliser la location par défaut. Certaines familles d'instances ne sont pas prises en charge dans la mesure où aucune autre taille n'est disponible. Pour plus d'informations, consultez Prise en charge de la modification de tailles d'instances .

Prérequis

Amazon EC2 traite votre demande de modification si votre capacité est suffisante pour votre nouvelle configuration (le cas échéant) et si les conditions suivantes sont respectées :

- Vous ne pouvez pas modifier la Instance réservée avant ou au moment même de son achat.
- La Instance réservée doit être active.
- Il ne peut pas y avoir de demande de modification en attente
- L'instance réservée n'est pas listée sur la marketplace des instances réservées.
- Il doit y avoir une correspondance entre la couverture de la taille de l'instance associée à la réservation initiale et la configuration cible. Pour plus d'informations, consultez [Prise en charge de la modification de tailles d'instances](#).

- Les instances réservées d'origine sont toutes des instances réservées standard ou des instances réservées convertibles, non pas quelques-unes de chaque sorte.
- Les instances réservées d'origine doivent expirer dans la même heure si ce sont des instances réservées standard.
- L'instance réservée n'est pas une instance G4, G4ad, G4dn, G5, G5g, Inf1 ou Inf2.

Prise en charge de la modification de tailles d'instances

Vous pouvez modifier la taille d'instance d'une Instance réservée si les conditions suivantes sont remplies.

Prérequis

- La plateforme est Linux/UNIX.
- Vous devez sélectionner une autre taille d'instance au sein de la même [famille d'instances](#) (indiquée par une lettre, par exemple T) et la même [génération](#) (indiquée par un chiffre, par exemple 2).

Par exemple, vous pouvez modifier une instance réservée de `t2.small` à `t2.large` parce qu'elles appartiennent toutes deux à la même famille et génération T2. Cependant, vous ne pouvez pas modifier une instance réservée de T2 à M2 ou de T2 à T3, car dans ces deux exemples, la famille et la génération d'instance cible ne sont pas les mêmes que celles de l'instance réservée d'origine.

- Vous ne pouvez pas modifier la taille d'instance des instances réservées pour les instances suivantes, car chacune d'entre elles n'a qu'une seule taille :
 - `t1.micro`
- Vous ne pouvez pas modifier la taille d'instance des instances réservées pour les combinaisons suivantes de famille d'instances, de génération et d'attribut :
 - G4ad
 - G4dn
 - G5
 - G5g
 - Inf1
 - Inf2
- Les Instance réservée nouvelle et d'origine doivent avoir la même couverture de taille d'instance.

Sommaire

- [Couverture de taille d'instance](#)
- [Facteur de normalisation pour les instances à matériel nu](#)

Couverture de taille d'instance

Chaque Instance réservée a une couverture de taille d'instance qui est déterminée par le facteur de normalisation de taille d'instance et par le nombre d'instances dans la réservation. Lorsque vous modifiez les tailles des instances dans une Instance réservée, la couverture de la nouvelle configuration doit correspondre à celle de la configuration d'origine, sinon la demande de modification n'est pas traitée.

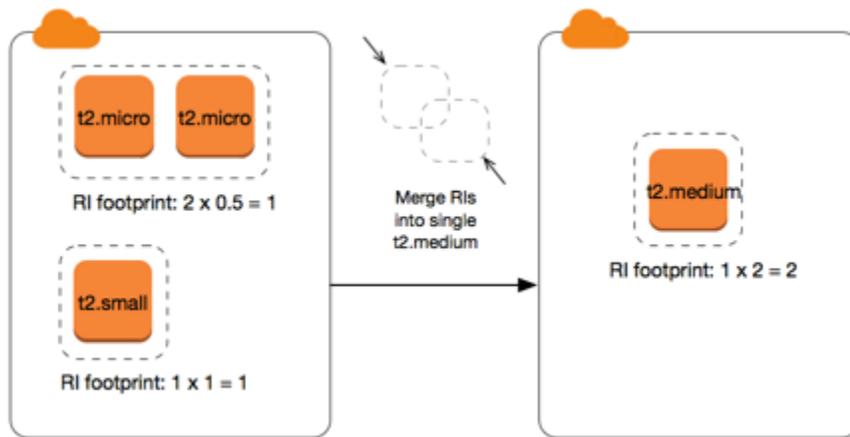
Pour calculer la couverture de la taille d'une Instance réservée, multipliez le nombre d'instances par le facteur de normalisation. Dans la console Amazon EC2, le facteur de normalisation est mesuré en unités. Le tableau suivant décrit le facteur de normalisation pour les tailles d'instance dans une famille d'instances. Par exemple, une instance `t2.medium` dispose d'un facteur de normalisation de 2, ce qui implique qu'une réservation de 4 instances `t2.medium` dispose d'une couverture de 8 unités.

Taille d'instance	Facteur de normalisation
nano	0.25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32

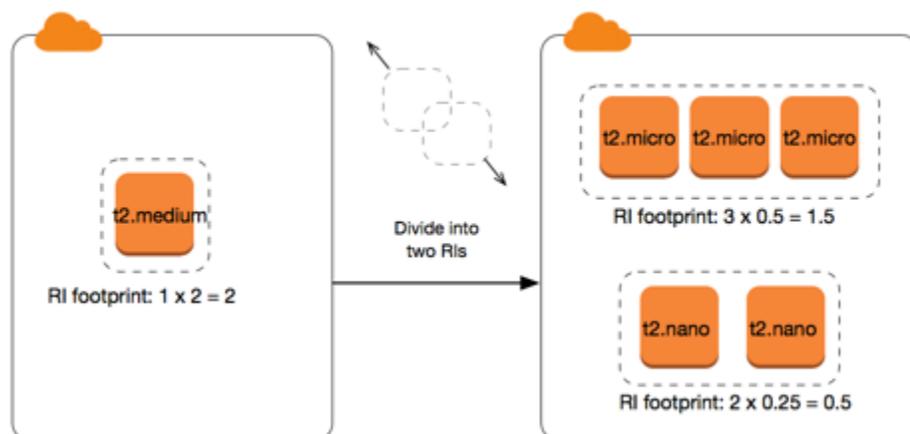
Taille d'instance	Facteur de normalisation
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Vous pouvez allouer vos réservations en utilisant différentes tailles d'instance sur la même famille de l'instance tant que la couverture de taille d'instance de votre réservation reste la même. Par exemple, vous pouvez diviser une réservation pour une instance `t2.large` (1 @ 4 unités) en quatre instances `t2.small` (4 @ 1 unité). De même, vous pouvez combiner une réservation pour quatre instances `t2.small` en une seule instance `t2.large`. Toutefois, vous ne pouvez pas remplacer votre réservation de deux instances `t2.small` par une seule instance `t2.large`, car la couverture de la nouvelle réservation (4 unités) est plus grande que celle de la réservation d'origine (2 unités).

Dans l'exemple suivant, vous avez une réservation avec deux instances `t2.micro` (1 unité) et une réservation avec une instance `t2.small` (1 unité). Si vous fusionnez ces deux réservations en une seule avec une instance `t2.medium` (2 unités), la couverture de la nouvelle réservation est égale à la couverture des réservations combinées.



Vous pouvez aussi modifier une réservation pour la diviser en deux réservations ou plus. Dans l'exemple suivant, vous disposez d'une réservation avec une instance `t2.medium` (2 unités). Vous pouvez diviser la réservation en deux, l'une avec deux instances `t2.nano` (0,5 unités) et l'autre avec trois instances `t2.micro` (1,5 unité).



Facteur de normalisation pour les instances à matériel nu

Vous pouvez modifier une réservation avec des instances `meta1` en utilisant d'autres tailles au sein de la même famille d'instances. De même, vous pouvez modifier une réservation avec des instances autres que des instances à matériel nu en utilisant la taille `meta1` de la même famille d'instances. Généralement, une instance à matériel nu a la même taille que la plus grande taille d'instance disponible au sein de la même famille d'instances. Par exemple, une instance `i3.meta1` a la même taille qu'une instance `i3.16xlarge`, de sorte qu'elles ont le même facteur de normalisation.

Le tableau suivant décrit le facteur de normalisation pour les tailles d'instance à matériel nu dans les familles d'instances qui ont des instances à matériel nu. Le facteur de normalisation des instances `meta1` dépend de la famille d'instances, contrairement aux autres tailles d'instance.

Taille d'instance	Facteur de normalisation
a1.metal	32
m5zn.metal x2iezn.metal z1d.metal	96
c6g.metal c6gd.metal i3.metal m6g.metal m6gd.metal r6g.metal r6gd.metal x2gd.metal	128
c5n.metal	144
c5.metal c5d.metal i3en.metal m5.metal m5d.metal m5dn.metal m5n.metal r5.metal r5b.metal r5d.metal r5dn.metal r5n.metal	192
c6i.metal c6id.metal m6i.metal m6id.metal r6d.metal r6id.metal	256
u-*.metal	896

Par exemple, une instance `i3.metal` dispose d'un facteur de normalisation de 128. Si vous achetez une Instance réservée Amazon Linux/Unix à location par défaut `i3.metal`, vous pouvez diviser la réservation comme suit :

- Une `i3.16xlarge` fait toujours la même taille qu'une instance `i3.metal`. Il dispose donc d'un facteur de normalisation de 128 (128/1). La réservation pour une instance `i3.metal` peut être modifiée en une instance `i3.16xlarge`.
- Une `i3.8xlarge` fait toujours la moitié de la taille d'une instance `i3.metal`. Il dispose donc d'un facteur de normalisation de 64 (128/2). La réservation pour une instance `i3.metal` peut être divisée en deux instances `i3.8xlarge`.
- Une `i3.4xlarge` fait toujours le quart de la taille d'une instance `i3.metal`. Il dispose donc d'un facteur de normalisation de 32 (128/4). La réservation pour une instance `i3.metal` peut être divisée en quatre instances `i3.4xlarge`.

Soumettre des demandes de modification

Avant de modifier vos instances réservées, assurez-vous d'avoir lu les [restrictions](#) applicables. Avant de modifier la taille de l'instance, calculez la [taille d'instance](#) totale des réservations d'origine que vous souhaitez modifier et assurez-vous qu'elle correspond à la taille d'instance totale de vos nouvelles configurations.

New console

Pour modifier vos instances réservées à l'aide du AWS Management Console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sur la page Instances réservées, sélectionnez une ou plusieurs Instances réservées à modifier, puis choisissez Actions, Modifier des instances réservées.

Note

Si vos Instances réservées ne sont pas actives ou si elles ne peuvent pas être modifiées, Modifier des Instances réservées est désactivé.

3. La première entrée du tableau de modification indique les attributs des instances réservées sélectionnées, et au moins une configuration cible en dessous. La colonne Unités indique la couverture de taille d'instance totale. Choisissez Ajouter pour chaque nouvelle configuration à ajouter. Modifiez les attributs de chaque configuration selon vos besoins.
 - Portée : indiquez si la configuration s'applique à une zone de disponibilité ou à l'ensemble de la région.
 - Zone de disponibilité : choisissez la zone de disponibilité requise. Ne s'applique pas aux instances réservées régionales.
 - Type d'instance : sélectionnez le type d'instance requis. Les configurations combinées doivent être égales à la couverture de taille d'instance de vos configurations d'origine.
 - Nombre : spécifiez le nombre d'instances. Pour fractionner les Instances réservées en plusieurs configurations, réduisez leur nombre, choisissez Ajouter et spécifiez un nombre pour la configuration supplémentaire. Par exemple, si vous disposez d'une configuration unique comportant 10 instances réservées, vous pouvez redéfinir ce nombre sur 6 et ajouter une configuration avec un nombre de 4. Ce processus supprime l'Instance réservée d'origine une fois les nouvelles instances réservées activées.
4. Choisissez Continue.

5. Pour valider vos choix de modification une fois que vous avez terminé la définition des configurations cibles, sélectionnez **Submit modifications** (Soumettre des modifications).
6. Vous pouvez consulter l'état de votre demande de modification en observant la colonne **État** de l'écran des Instances réservées. Les états possibles sont les suivants :
 - **active** (en attente de modification) : État de transition pour les Instances réservées initiales
 - **hors service** (en attente de modification) : État de transition pour les Instances réservées initiales pendant que les nouvelles Instances réservées sont créées
 - **hors service** : Instances réservées modifiées et remplacées avec succès.
 - **active** : L'un des statuts suivants :
 - Nouvelles instances réservées créées à la suite d'une demande de modification
 - instances réservées initiales après l'échec d'une demande de modification

Old console

Pour modifier vos instances réservées à l'aide du AWS Management Console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sur la page Instances réservées, sélectionnez une ou plusieurs Instances réservées à modifier, puis choisissez **Actions**, **Modifier des instances réservées**.

Note

Si vos Instances réservées ne sont pas actives ou si elles ne peuvent pas être modifiées, **Modifier des Instances réservées** est désactivé.

3. La première entrée du tableau de modification indique les attributs des instances réservées sélectionnées, et au moins une configuration cible en dessous. La colonne **Unités** indique la couverture de taille d'instance totale. Choisissez **Ajouter** pour chaque nouvelle configuration à ajouter. Modifiez les attributs de chaque configuration selon vos besoins, puis choisissez **Continuer** :
 - **Portée** : indiquez si la configuration s'applique à une zone de disponibilité ou à l'ensemble de la région.
 - **Zone de disponibilité** : choisissez la zone de disponibilité requise. Ne s'applique pas aux instances réservées régionales.

- Type d'instance : sélectionnez le type d'instance requis. Les configurations combinées doivent être égales à la couverture de taille d'instance de vos configurations d'origine.
 - Nombre : spécifiez le nombre d'instances. Pour fractionner les Instances réservées en plusieurs configurations, réduisez leur nombre, choisissez Ajouter et spécifiez un nombre pour la configuration supplémentaire. Par exemple, si vous disposez d'une configuration unique comportant 10 instances réservées, vous pouvez redéfinir ce nombre sur 6 et ajouter une configuration avec un nombre de 4. Ce processus supprime l'Instance réservée d'origine une fois les nouvelles instances réservées activées.
4. Pour valider vos choix de modification une fois que vous avez terminé la définition des configurations cibles, sélectionnez Submit modifications (Soumettre des modifications).
 5. Vous pouvez consulter l'état de votre demande de modification en observant la colonne État de l'écran des Instances réservées. Les états possibles sont les suivants :
 - active (en attente de modification) : État de transition pour les Instances réservées initiales
 - hors service (en attente de modification) : État de transition pour les Instances réservées initiales pendant que les nouvelles Instances réservées sont créées
 - hors service : Instances réservées modifiées et remplacées avec succès.
 - active : L'un des statuts suivants :
 - Nouvelles instances réservées créées à la suite d'une demande de modification
 - instances réservées initiales après l'échec d'une demande de modification

Pour modifier vos instances réservées à l'aide de la ligne de commande

1. Pour modifier vos instances réservées, vous pouvez utiliser l'une des commandes suivantes :
 - [modify-reserved-instances](#) (AWS CLI)
 - [Edit-EC2ReservedInstance](#) (AWS Tools for Windows PowerShell)
2. Pour obtenir le statut de votre demande modification (processing, fulfilled ou failed), utilisez une des commandes suivantes :
 - [describe-reserved-instances-modifications](#) (AWS CLI)
 - [Get-EC2ReservedInstancesModification](#) (AWS Tools for Windows PowerShell)

Résoudre les problèmes liés aux demandes de modification

Si les paramètres que vous avez demandés pour la configuration cible sont uniques, vous recevez un message indiquant que votre demande est en cours de traitement. A ce stade, Amazon EC2 a uniquement déterminé que les paramètres de votre demande de modification étaient valides. Votre demande de modification peut encore échouer au cours du traitement si la capacité nécessaire n'est pas disponible.

Dans certains cas, vous ne recevrez pas de confirmation, mais un message indiquant que la demande de modification a échoué ou est incomplète. Utilisez les informations de ces messages comme point de départ pour soumettre une nouvelle demande de modification. Veillez à lire les [restrictions](#) applicables avant d'envoyer la demande.

Certaines instances réservées sélectionnées ne peuvent pas faire l'objet d'une modification

Amazon EC2 identifie et répertorie les instances réservées qui ne peuvent pas être modifiées. Si vous recevez un message de ce type, accédez à la page Instances réservées de la console Amazon EC2 et consultez les informations pour les Instances réservées.

Erreur lors du traitement de votre demande de modification

Vous avez demandé la modification d'une ou de plusieurs instances réservées, mais aucune de ces demandes ne peut être traitée. Selon le nombre de réservations que vous modifiez, vous pouvez obtenir différentes versions de ce message.

Amazon EC2 affiche les raisons pour lesquelles votre demande ne peut pas être traitée. Par exemple, vous pouvez avoir spécifié la même configuration cible (une combinaison de zone de disponibilité et de plateforme) pour une ou plusieurs parties des instances réservées que vous modifiez. Essayez de soumettre à nouveau les demandes de modification, mais veillez à ce que les détails d'instance des réservations soient corrects et à ce que les configurations cibles pour toutes les parties modifiées soient uniques.

Échanger des instances réservées convertibles

Vous pouvez échanger une ou plusieurs instances réservées convertibles contre une autre Instance réservée convertible avec une configuration différente, y compris la famille de l'instance, le système d'exploitation et la location. Il n'y a pas de limite au nombre d'échanges que vous pouvez effectuer, tant que l'Instance réservée convertible nouvelle est de valeur égale ou plus élevée que les instances réservées convertibles que vous échangez.

Lorsque vous échangez votre instance réservée convertible, le nombre d'instances de votre réservation actuelle est remplacé par un nombre d'instances qui couvre une valeur égale ou supérieure à celle de la configuration de la nouvelle instance réservée convertible. Amazon EC2 calcule le nombre d'instances réservées que vous pouvez recevoir à la suite de l'échange.

Vous ne pouvez pas échanger d'instances réservées standard, mais vous pouvez les modifier. Pour plus d'informations, consultez [Modifier instances réservées](#).

Sommaire

- [Exigences pour l'échange d'instances réservées convertibles](#)
- [Calculer des échanges d'instances réservées convertibles](#)
- [Fusionner des instances réservées convertibles](#)
- [Échanger une partie d'une Instance réservée convertible](#)
- [Soumettre des demandes d'échange](#)

Exigences pour l'échange d'instances réservées convertibles

Si les conditions suivantes sont remplies, Amazon EC2 traite votre demande d'échange. Votre Instance réservée convertible doit être :

- Actif
- Libre de toute demande d'échange précédente
- Il doit rester au moins 24 heures avant son expiration

Les règles suivantes s'appliquent :

- Les instances réservées convertibles ne peuvent être échangées que contre d'autres instances réservées convertibles actuellement proposées par AWS.
- Les instances réservées convertibles sont associées à une région spécifique, qui reste la même pendant la durée de la période de réservation. Vous ne pouvez pas échanger une Instance réservée convertible par une Instance réservée convertible d'une autre région.
- Vous pouvez échanger une ou plusieurs instances réservées convertibles à la fois contre une seule Instance réservée convertible.
- Pour échanger une partie d'une Instance réservée convertible, vous pouvez la modifier en deux réservations ou plus, avant d'en échanger une ou plusieurs contre une nouvelle Instance réservée

convertible. Pour plus d'informations, consultez [Échanger une partie d'une Instance réservée convertible](#). Pour plus d'informations sur la modification de vos Instances réservées, consultez [Modifier instances réservées](#).

- Les instances réservées convertibles avec tous les frais initiaux peuvent être échangées contre des instances réservées convertibles avec frais initiaux partiels, et inversement.

 Note

Si le paiement total des frais initiaux requis pour l'échange (coût de régularisation) est inférieur à 0,00 USD, AWS vous donne automatiquement une quantité d'instances parmi les instances réservées convertibles qui garantit que le coût de régularisation est de 0,00 USD ou plus.

 Note

Si la valeur totale (prix initial + prix horaire* nombre d'heures restantes) de la nouvelle instance réservée convertible est inférieure à la valeur totale de l'instance réservée convertible échangée, vous obtenez AWS automatiquement une quantité d'instances dans l'instance réservée convertible qui garantit que la valeur totale est égale ou supérieure à celle de l'instance réservée convertible échangée.

- Pour bénéficier d'un meilleur tarif, vous pouvez échanger une Instance réservée convertible sans paiement initial pour une Instance réservée convertible avec tous les frais totaux ou avec frais initiaux partiels.
- Vous ne pouvez pas échanger de instances réservées convertibles avec tous les frais initiaux ou avec frais initiaux partiels contre des instances réservées convertibles. sans frais initiaux.
- Vous pouvez échanger une Instance réservée convertible sans frais initiaux pour une autre Instance réservée convertible sans frais initiaux uniquement si le tarif horaire de la nouvelle Instance réservée convertible est égal ou supérieur au prix horaire de la Instance réservée convertible échangée.

 Note

Si la valeur totale (prix horaire* nombre d'heures restantes) de la nouvelle instance réservée convertible est inférieure à la valeur totale de l'instance réservée convertible échangée, vous obtenez AWS automatiquement une quantité d'instances dans l'instance

réservée convertible qui garantit que la valeur totale est égale ou supérieure à celle de l'instance réservée convertible échangée.

- Si vous échangez plusieurs instances réservées convertibles avec différentes dates d'expiration, la date d'expiration de la nouvelle instance réservée convertible est la plus lointaine dans le futur.
- Si vous échangez une Instance réservée convertible unique, elle doit avoir la même durée que la nouvelle Instance réservée convertible (1 an ou 3 ans). Si vous fusionnez plusieurs instances réservées convertibles avec différentes durées, la nouvelle Instance réservée convertible aura une durée de 3 ans. Pour plus d'informations, consultez [Fusionner des instances réservées convertibles](#).
- Lorsqu'Amazon EC2 échange une instance réservée convertible, il retire la réservation associée et transfère la date de fin à la nouvelle réservation. Après l'échange, Amazon EC2 fixe à la fois la date de fin de l'ancienne réservation et la date de début de la nouvelle réservation correspondant à la date de l'échange. Par exemple, si vous échangez une réservation d'une durée de trois ans avec 16 mois restants, la nouvelle réservation a une durée de 16 mois, avec la même date de fin que la réservation de l'instance réservée convertible que vous avez échangée.

Calculer des échanges d'instances réservées convertibles

L'échange de instances réservées convertibles est gratuit. Toutefois, vous pouvez être tenu de payer des frais de régularisation calculés au prorata du paiement comptant de la différence entre les instances réservées convertibles que vous aviez et les nouvelles instances réservées convertibles que vous recevez de l'échange.

Chaque Instance réservée convertible dispose d'une liste de valeurs. Cette valeur de liste est comparée à la valeur de liste des instances réservées convertibles que vous voulez pour déterminer combien de réservations d'instances vous pouvez recevoir de l'échange.

Par exemple : vous avez une Instance réservée convertible avec une valeur de liste de 35 \$ que vous voulez échanger contre un nouveau type d'instance avec une valeur de liste de 10 USD.

$$\$35/\$10 = 3.5$$

Vous pouvez échanger votre Instance réservée convertible contre trois instances réservées convertibles de 10 USD. Étant donné qu'il n'est pas possible d'acheter des moitiés de réservation, vous devez acheter une Instance réservée convertible supplémentaire pour couvrir le reste :

3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved Instance

La quatrième Instance réservée convertible a la même date de fin que les trois autres. Vous payez la régularisation correspondant à la quatrième réservation si vous échangez des instances réservées convertibles à paiement initial partiel ou comptant. Si le reste du paiement en amont de vos instances réservées convertibles est de 500 USD et que la nouvelle réservation coûterait normalement 600 USD au prorata, vous êtes facturé 100 USD.

$\$600$ prorated upfront cost of new reservations - $\$500$ remaining upfront cost of old reservations = $\$100$ difference

Fusionner des instances réservées convertibles

Si vous fusionnez deux instances réservées convertibles ou plus, le terme de l'instance réservée convertible obtenue doit être le même que celui des instances réservées convertibles ou celui de la plus grande des instances réservées convertibles. La date d'expiration de la nouvelle Instance réservée convertible est la plus lointaine dans le futur.

Par exemple, si vous possédez les instances réservées convertibles suivantes sur votre compte :

ID Instance réservée	Durée	Date d'expiration
aaaa1111	1 an	31-12-2018
bbbb2222	1 an	31-07-2018
cccc3333	3 ans	30-06-2018
dddd4444	3 ans	31-12-2019

- Vous pouvez fusionner aaaa1111 et bbbb2222 et les échanger contre une Instance réservée convertible valable 1 an. Vous ne pouvez pas les échanger contre une Instance réservée convertible valable trois ans. La date d'expiration de la nouvelle Instance réservée convertible est 2018-12-31.
- Vous pouvez fusionner bbbb2222 et cccc3333 et les échanger contre une Instance réservée convertible valable 3 ans. Vous ne pouvez pas les échanger contre une Instance réservée

convertible valable un an. La date d'expiration de la nouvelle Instance réservée convertible est 2018-07-31.

- Vous pouvez fusionner cccc3333 et dddd4444 et les échanger contre une Instance réservée convertible valable 3 ans. Vous ne pouvez pas les échanger contre une Instance réservée convertible valable un an. La date d'expiration de la nouvelle Instance réservée convertible est 2019-12-31.

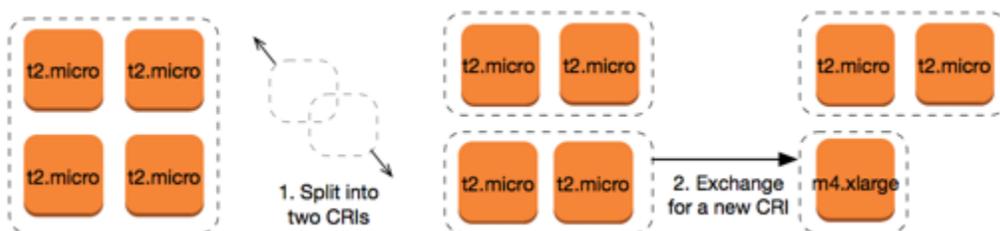
Échanger une partie d'une Instance réservée convertible

Vous pouvez utiliser le processus de modification pour diviser votre Instance réservée convertible en plus petites réservations, avant d'en échanger une ou plusieurs contre une nouvelle Instance réservée convertible. Les exemples suivant montrent comment procéder.

Exemple Exemple : Instance réservée convertible avec plusieurs instances

Dans cet exemple, vous disposez d'une Instance réservée convertible `t2.micro` avec quatre instances dans la réservation. Pour échanger deux instances `t2.micro` contre une instance `m4.xlarge` :

1. Modifiez la Instance réservée convertible `t2.micro` en la divisant en deux Instances réservées convertibles `t2.micro` avec deux instances chacune.
2. Échangez l'une des nouvelles Instances réservées convertibles `t2.micro` obtenues contre une Instance réservée convertible `m4.xlarge`.

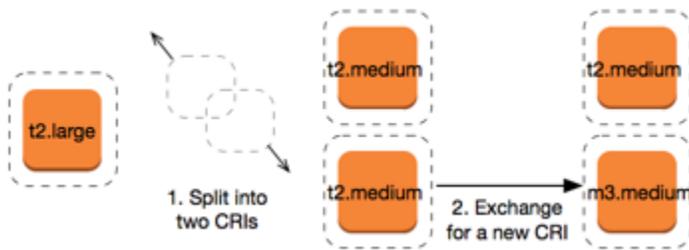


Exemple Exemple : Instance réservée convertible avec une seule instance

Dans cet exemple, vous disposez d'une `t2.large` Instance réservée convertible. Pour la changer en une instance `t2.medium` plus petite et une instance `m3.medium` :

1. Modifiez l'Instance réservée convertible `t2.large` en la divisant en deux Instances réservées convertibles `t2.medium`. Une seule instance `t2.large` a la même couverture de taille d'instance que les deux instances `t2.medium`.

- Échangez l'une des nouvelles Instances réservées convertibles t2.medium obtenues contre une Instance réservée convertible m3.medium.



Pour plus d'informations, consultez [Prise en charge de la modification de tailles d'instances](#) et [Soumettre des demandes d'échange](#).

Soumettre des demandes d'échange

Vous pouvez échanger vos instances réservées convertibles à l'aide de la console Amazon EC2 ou d'un outil de ligne de commande.

Échanger une Instance réservée convertible à l'aide de la console

Vous pouvez rechercher des offres de instances réservées convertibles et sélectionner votre nouvelle configuration parmi les choix fournis.

New console

Pour échanger des instances réservées convertibles à l'aide de la console Amazon EC2 :

- Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
- Choisissez Instances réservées, sélectionnez les Instances réservées convertibles à échanger, puis choisissez Actions, Échange de l'Instance réservée.
- Sélectionnez les attributs de la configuration souhaitée et sélectionnez Find offering (Trouver une offre).
- Sélectionnez une nouvelle Instance réservée convertible. En bas de l'écran, vous pouvez consulter le nombre de instances réservées que vous recevez pour l'échange, ainsi que les éventuels coûts supplémentaires.
- Lorsque vous avez sélectionné une Instance réservée convertible qui répond à vos besoins, sélectionnez Review (Vérifier).
- Sélectionnez Exchange (Échange), puis Close (Fermer).

Old console

Pour échanger des instances réservées convertibles à l'aide de la console Amazon EC2 :

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Instances réservées, sélectionnez les Instances réservées convertibles à échanger, puis choisissez Actions, Échange de l'Instance réservée.
3. Sélectionnez les attributs de la configuration souhaitée et sélectionnez Find Offering (Trouver une offre).
4. Sélectionnez une nouvelle Instance réservée convertible. La colonne Instance Count (Nombre d'instances) indique le nombre d'Instances réservées que vous recevez pour l'échange. Lorsque vous avez sélectionné une Instance réservée convertible qui répond à vos besoins, choisissez Échange.

Les instances réservées qui ont été échangées sont mises hors service et les nouvelles instances réservées s'affichent dans la console Amazon EC2. Ce processus peut prendre quelques minutes pour se propager.

Échanger une instance réservée convertible à l'aide de l'interface de la ligne de commande

Pour échanger une Instance réservée convertible, commencez par rechercher une nouvelle Instance réservée convertible qui répond à vos besoins :

- [describe-reserved-instances-offerings](#) (AWS CLI)
- [Get-EC2ReservedInstancesOffering](#)(Outils pour Windows PowerShell)

Obtenez un devis pour l'échange, qui inclut le nombre de instances réservées que vous obtenez lors de l'échange et les frais de régularisation pour l'échange :

- [get-reserved-instances-exchange-quote](#) (AWS CLI)
- [GetEc2- ReservedInstances ExchangeQuote](#) (Outils pour Windows) PowerShell

Enfin, effectuez l'échange :

- [accept-reserved-instances-exchange-quote](#) (AWS CLI)
- [Confirm-EC2ReservedInstancesExchangeQuote](#)(Outils pour Windows PowerShell)

Quotas d'instances réservées

Vous pouvez acheter de nouvelles instances réservées chaque mois. Le nombre de nouvelles instances réservées que vous pouvez acheter chaque mois est déterminé par votre quota mensuel, comme indiqué ci-dessous :

Description du quota	Quota par défaut
Nouvelles instances réservées régionales	20 par région et par mois
Nouvelles instances réservées zonales	20 par zone de disponibilité et par mois

Par exemple, dans une région comportant trois zones de disponibilité, le quota par défaut est de 80 nouvelles instances réservées par mois, calculé comme suit :

- 20 instances réservées régionales pour la région
- Plus 60 instances réservées zonales (20 pour chacune des trois zones de disponibilité)

Les instances de l'état `running` sont prises en compte dans votre quota. Les instances situées dans les états `hibernated`, `pending`, `stopping` et `stopped`, et ne sont pas prises en compte dans votre quota.

Afficher le nombre total d'instances réservées que vous avez achetées

Le nombre d'instances réservées que vous achetez est indiqué par le champ Instance count (Nombre d'instances, console) ou par le paramètre InstanceCount (AWS CLI). Lorsque vous achetez de nouvelles instances réservées, le quota est mesuré par rapport au nombre total d'instances. Par exemple, si vous achetez une configuration d'instance réservée unique avec un nombre d'instances de 10, l'achat compte dans votre quota à 10, et non à 1.

Vous pouvez consulter le nombre d'instances réservées que vous avez achetées en utilisant Amazon EC2 ou l' AWS CLI.

Console

Pour afficher le nombre total d'instances réservées que vous avez achetées

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Reserved Instances (Instances réservées).

- Sélectionnez une configuration d'instance réservée dans le tableau, puis vérifiez le champ Instance count (Nombre d'instances).

Dans la capture d'écran suivante, la ligne sélectionnée représente une configuration d'instance réservée unique pour un type d'instance `t3.micro`. La colonne Instance count (Nombre d'instances) de la vue de table et le champ Instance count de la vue détaillée (mis en évidence dans la capture d'écran) indiquent qu'il existe 10 instances réservées pour cette configuration.

The screenshot shows the AWS Management Console interface for Reserved Instances. At the top, there's a breadcrumb 'EC2 > Reserved Instances' and a title 'Reserved Instances (32) Info'. Below the title is a search bar and a 'Purchase Reserved Instances' button. A table lists reserved instances with columns: Instance ty..., Scope, Availabilit..., Instance count, Start, Expires, and Offering cl... The first row is selected, showing 't3.micro' instance type, 'Region' scope, and '10' instance count. Below the table, a summary bar indicates '1 Reserved Instance selected'. The 'Details' view is open, showing a grid of instance attributes. The 'Instance count' field in the details view is highlighted with a red box, showing a value of '10'.

Instance ty...	Scope	Availabilit...	Instance count	Start	Expires	Offering cl...
<input checked="" type="checkbox"/> t3.micro	Region	-	10	August 27, 2022, 15:29 (UTC+2:00)	August 27, 2023, 15:29 (UTC+2:00)	Standard
<input type="checkbox"/> t3.micro	Region	-	4	November 8, 2021, 14:19 (UTC+2:00)	November 8, 2022, 14:19 (UTC+2:00)	Standard

1 Reserved Instance selected

Reserved Instance ID: 2fbf16dd-98b6-4a3a-955f-83f87790f04b Info

Instance type <input checked="" type="checkbox"/> t3.micro	Scope <input checked="" type="checkbox"/> Region	Instance count <input checked="" type="checkbox"/> 10	Availability Zone -
Start <input checked="" type="checkbox"/> August 27, 2022, 15:29 (UTC+2:00)	Platform <input checked="" type="checkbox"/> Linux/UNIX	Expires <input checked="" type="checkbox"/> August 27, 2023, 15:29 (UTC+2:00)	Term <input checked="" type="checkbox"/> 1 year
Payment option <input checked="" type="checkbox"/> All upfront	Time left <input checked="" type="checkbox"/> around 50 weeks 6 days	Upfront price <input checked="" type="checkbox"/> \$59.00	Offering class <input checked="" type="checkbox"/> Standard
Usage price <input checked="" type="checkbox"/> \$0.00	State <input checked="" type="checkbox"/> Active	Hourly charges <input checked="" type="checkbox"/> \$0.00	Tenancy <input checked="" type="checkbox"/> Default

AWS CLI

Pour afficher le nombre total d'instances réservées que vous avez achetées

Utilisez la commande CLI [describe-reserved-instances](#) et spécifiez l'ID de la configuration d'instance réservée.

```
aws ec2 describe-reserved-instances \
  --reserved-instances-ids 2fbf16dd-98b6-4a3a-955f-83f87790f04b \
  --output table
```

Exemple de sortie : le champ InstanceCount indique qu'il existe 10 instances réservées pour cette configuration.

```

| DescribeReservedInstances |
+-----+
|| ReservedInstances ||
|+-----+|
|| CurrencyCode | USD ||
|| Duration | 31536000 ||
|| End | 2023-08-27T13:29:44+00:00 ||
|| FixedPrice | 59.0 ||
|| InstanceCount | 10 ||
|| InstanceTenancy | default ||
|| InstanceType | t3.micro ||
|| OfferingClass | standard ||
|| OfferingType | All Upfront ||
|| ProductDescription | Linux/UNIX ||
|| ReservedInstancesId | 2fbf16dd-98b6-4a3a-955f-83f87790f04b ||
|| Scope | Region ||
|| Start | 2022-08-27T13:29:45.938000+00:00 ||
|| State | active ||
|| UsagePrice | 0.0 ||
|+-----+|
||| RecurringCharges ||| |
||+-----+||
||| Amount | 0.0 |||
||| Frequency | Hourly |||
||+-----+||

```

Considérations

Une Instance réservée régionale applique une remise à une instance à la demande en cours d'exécution. La limite d'instance à la demande par défaut est de 20. Vous ne pouvez pas dépasser votre limite d'instance à la demande en cours d'exécution en achetant des instances réservées régionales. Par exemple, si vous avez déjà 20 instances à la demande en cours d'exécution, et que vous achetez 20 instances réservées régionales, les 20 instances réservées régionales sont utilisées pour appliquer une remise aux 20 instances à la demande en cours d'exécution. Si vous achetez plus d'instances réservées régionales, vous ne pourrez pas lancer plus d'instances flottee que vous avez atteint votre limite d'instance à la demande.

Avant d'acheter des instances réservées régionales, assurez-vous que votre limite d'instance à la demande atteint ou dépasse le nombre d'instances réservées régionales que vous comptez posséder. Si nécessaire, assurez-vous de demander une augmentation de votre limite d'instance à la demande avant d'acheter des Instances réservées régionales supplémentaires.

Une instance réservée zonale, c'est-à-dire une instance réservée achetée pour une zone de disponibilité spécifique, offre une réserve de capacité ainsi qu'une remise. Vous pouvez dépasser votre limite d'instance à la demande en cours d'exécution en achetant des Instances réservées zonales. Par exemple, si vous avez déjà 20 instances à la demande en cours d'exécution et que vous achetez 20 instances réservées zonales, vous pouvez lancer 20 instances à la demande supplémentaires qui correspondent aux spécifications de vos instances réservées zonales, ce qui vous donne un total de 40 instances en cours d'exécution.

Afficher vos quotas d'instances réservées et demander une augmentation de quota

La console Amazon EC2 indique des informations relatives aux quotas. Vous pouvez également demander une augmentation de vos quotas. Pour plus d'informations, consultez [Afficher vos quotas actuels](#) et [Demander une augmentation](#).

Spot instances

Une instance Spot est une instance qui utilise la capacité EC2 inutilisée disponible à un prix inférieur au prix d'une A la demande. Comme une instances Spot vous permet de demander des instances EC2 inutilisées avec de fortes remises, vous pouvez réduire considérablement vos coûts Amazon EC2. Le prix horaire d'une instance Spot est appelé prix spot. Le prix Spot de chaque type d'instance dans chaque zone de disponibilité est défini par Amazon EC2 et varie en fonction de l'offre et de la demande à long terme pour les instances Spot. Votre instance Spot s'exécute chaque fois que la capacité est disponible.

Les instances Spot constituent un choix économique si vous êtes flexible quant au moment où vos applications s'exécutent et à la possibilité de les interrompre. Par exemple, les instances Spot sont particulièrement adaptées à l'analyse de données, aux travaux par lots, au traitement en arrière-plan et aux tâches facultatives. Pour plus d'informations, consultez [Amazon EC2 Instances Spot](#).

Pour une comparaison des différentes options d'achat des instances EC2, consultez [Options d'achat d'instance](#).

Rubriques

- [Concepts](#)
- [Comment démarrer](#)
- [Services connexes](#)
- [Tarification et économies](#)

Concepts

Avant de commencer à utiliser les instances Spot, vous devez connaître les concepts suivants :

- Groupe de capacités Spot – Un ensemble d'instances EC2 inutilisées avec le même type d'instance (par exemple, `m5.Large`) et la même zone de disponibilité.
- Prix Spot – Prix horaire actuel d'une instance Spot.
- Demande d'instance Spot – Demande d'une instance Spot. Lorsque la capacité est disponible, Amazon EC2 répond à votre demande. Une demande d'instance Spot est soit One-time (Unique) soit Persistent (Persistante). Amazon EC2 soumet à nouveau automatiquement une demande d'Instance Spot persistante après que l'Instance Spot associée à la demande soit interrompue.

- **Recommandation de rééquilibrage d'instance EC2** – Amazon EC2 émet un signal de recommandation de rééquilibrage d'instance pour vous avertir qu'une instance Spot présente un risque élevé d'interruption. Ce signal vous donne la possibilité de rééquilibrer de manière proactive vos charges de travail entre les instances Spot existantes ou nouvelles sans avoir à attendre l'avis d'interruption d'instance Spot deux minutes avant celle-ci.
- **Spot Instance interruption (Interruption d'instance Spot)** – Amazon EC2 résilie, arrête ou met en veille prolongée votre instance Spot lorsque Amazon EC2 a besoin de récupérer la capacité. Amazon EC2 communique un avis d'interruption d'instance Spot, qui donne à l'instance un avertissement deux minutes avant qu'elle soit interrompue.

Principales différences entre les instances Spot et les instances à la demande

Le tableau suivant répertorie les principales différences entre les instances Spot et les [instances à la demande](#).

	Spot instances	On-Demand instances
Heure de lancement	Ne peut être lancée immédiatement que si la demande d'instance Spot est active et la capacité disponible.	Peut uniquement être lancé immédiatement si vous émettez une demande de lancement manuel et que la capacité est disponible.
Capacité disponible	Si la capacité n'est pas disponible, la demande d'instance Spot continue à effectuer automatiquement la demande de lancement jusqu'à ce que la capacité devienne disponible.	Si la capacité n'est pas disponible lorsque vous effectuez une demande de lancement, vous obtenez une erreur de capacité insuffisante (ICE).
Tarif horaire	Le prix horaire pour les instances Spot varie en fonction de l'offre et de la demande à long terme.	Le prix horaire pour les instances à la demande est statique.
Recommandation de rééquilibrage	Le signal émis par Amazon EC2 pour une instance Spot exécutée lorsque	Vous déterminez le moment où une instance à la demande est interrompue

	Spot instances	On-Demand instances
	l'instance présente un risque élevé d'interruption.	(arrêtée, mise en veille prolongée ou résiliée).
Interruption d'instance	Vous pouvez arrêter et démarrer une instance Spot basée sur Amazon EBS. En outre, Amazon EC2 peut interrompre une instance Spot individuelle si la capacité n'est plus disponible.	Vous déterminez le moment où une instance à la demande est interrompue (arrêtée, mise en veille prolongée ou résiliée).

Comment démarrer

Vous devez commencer par préparer l'utilisation d'Amazon EC2. Il peut être utile d'avoir déjà eu l'occasion de lancer des instances à la demande avant de lancer des instances Spot.

Bases des instances Spot

- [Fonctionnement des instances Spot](#)

Utilisation de instances Spot

- [Créer une demande d'instance Spot](#)
- [Obtenir des informations sur le statut d'une demande](#)
- [Interruptions d'instance Spot](#)

Services connexes

Vous pouvez allouer des instances Spot directement à partir d'Amazon EC2. Vous pouvez également allouer des instances Spot à partir d'autres services dans AWS. Pour plus d'informations, consultez la documentation suivante.

Amazon EC2 Auto Scaling et instances Spot

Vous pouvez créer des modèles ou des configurations de lancement de façon à ce qu'Amazon EC2 Auto Scaling puisse lancer des instances Spot. Pour plus d'informations, consultez les sections [Demande d'Instances Spot pour des applications flexibles et tolérantes aux pannes](#) et

[Groupes Auto Scaling avec plusieurs types d'instance et options d'achat](#) du Amazon EC2 Auto Scaling Guide de l'utilisateur.

Amazon EMR et instances Spot

Dans certains cas de figure, il peut être utile d'exécuter des instances Spot dans un cluster Amazon EMR. Pour plus d'informations, consultez [Instances Spot](#) et [Quand faut-il utiliser des Instances Spot ?](#) dans le Amazon EMR Guide de gestion.

AWS CloudFormation modèles

AWS CloudFormation vous permet de créer et de gérer un ensemble de AWS ressources à l'aide d'un modèle au format JSON. Pour plus d'informations, consultez [EC2 Spot Instance Updates - Auto Scaling and CloudFormation Integration](#).

AWS SDK for Java

Vous pouvez utiliser le langage de programmation Java afin de gérer vos instances Spot. Pour plus d'informations, consultez [Didacticiel : instances Spot Amazon EC2](#) et [Didacticiel : Gestion avancée des demandes Spot Amazon EC2](#).

AWS SDK for .NET

Vous pouvez utiliser l'environnement de programmation .NET pour gérer vos instances Spot. Pour plus d'informations, consultez [Didacticiel : Instances Spot Amazon EC2](#).

Tarifcation et économies

Vous payez le prix spot des instances Spot qui est défini par Amazon EC2 et varie régulièrement en fonction de l'offre et de la demande à long terme pour les instances Spot. Vos Instances Spot sont exécutées jusqu'à ce que vous les résilieez, dès que la capacité n'est plus disponible ou que votre groupe Amazon EC2 Auto Scaling les résilie durant la [mise à l'échelle horizontale](#).

Si vous-même ou Amazon EC2 interrompez une instance Spot en cours d'exécution, vous serez facturé pour les secondes utilisées ou l'heure complète, ou vous ne serez pas facturé, selon le système d'exploitation utilisé et qui a interrompu l'instance Spot. Pour plus d'informations, consultez [Facturation des instances Spot interrompues](#).

Les instances Spot ne sont pas couvertes par Savings Plans. Si vous avez un Savings Plan, celui-ci ne vous permet pas de réaliser des économies supplémentaires en plus des économies déjà réalisées en utilisant les instances Spot. De plus, vos dépenses pour les instances Spot n'appliquent pas les engagements de vos Compute Savings Plans.

Consulter les tarifs

Pour connaître le prix spot le plus bas actuel (mis à jour toutes les cinq minutes) par type Région AWS d'instance, consultez la page de [tarification des instances ponctuelles Amazon EC2](#).

Pour consulter l'historique du prix Spot au cours des trois derniers mois, utilisez la console Amazon EC2 ou la commande [describe-Spot-price-history](#) (AWS CLI). Pour plus d'informations, consultez [Historique de tarification d'instances Spot](#).

Nous mappons indépendamment les zones de disponibilité aux codes de chacune d'entre elles Compte AWS. Par conséquent, vous pouvez obtenir des résultats variables pour un même code de zone de disponibilité (par exemple, us-west-2a) entre différents comptes.

Consulter les économies

Vous pouvez afficher les économies réalisées grâce à l'utilisation d'instances Spot pour un seul [parc d'instances Spot](#) ou pour toutes les instances Spot. Vous pouvez consulter les économies réalisées au cours de la dernière heure ou des trois derniers jours, ainsi que le coût moyen par heure vCPU et par heure de mémoire (Gio). Les économies sont des estimations et peuvent différer de vos économies réelles, car elles ne tiennent pas compte des ajustements de facturation en fonction de votre utilisation. Pour plus d'informations sur la consultation des informations sur les économies, consultez [Économies réalisées grâce à l'achat d'instances Spot](#).

Consulter les factures

Votre facture fournit des détails sur votre utilisation du service. Pour plus d'informations, consultez la section [Viewing your bill](#) (Affichage d'une facture) dans le Guide de l'utilisateur AWS Billing .

Bonnes pratiques pour EC2 Spot

Les instances Spot Amazon EC2 sont des capacités de calcul EC2 inutilisées mises à votre disposition avec des économies allant jusqu'à 90 % par rapport aux prix à la demande. AWS Cloud La seule différence entre les instances à la demande et les instances Spot est que les instances Spot peuvent être interrompues par Amazon EC2, avec deux minutes de préavis, quand Amazon EC2 a besoin de récupérer la capacité.

Les instances Spot sont recommandés pour les applications flexibles sans état, tolérantes aux pannes. Par exemple, instances Spot fonctionne bien pour le Big Data, les charges de travail conteneurisées, les CI/CD, les serveurs Web sans état, le calcul haute performance (HPC) et les charges de travail de rendu.

En cours d'exécution, les instances Spot sont exactement les mêmes que instances à la demande. Toutefois, Spot ne garantit pas que vous pouvez conserver vos instances en cours d'exécution suffisamment longtemps pour terminer vos charges de travail. Spot ne garantit pas non plus que vous pouvez obtenir la disponibilité immédiate des instances que vous recherchez, ou que vous pouvez toujours obtenir la capacité globale que vous avez demandée. De plus, les interruptions et la capacité des instances Spot peuvent changer au fil du temps, car leur disponibilité varie en fonction de l'offre et de la demande, et les performances passées ne sont pas une garantie de résultats futurs.

Les instances Spot ne conviennent pas aux charges de travail inflexibles, dynamiques, intolérantes aux pannes ou étroitement couplées entre des nœuds d'instance. Nous ne recommandons pas les instances Spot pour les charges de travail qui ne tolèrent pas les périodes occasionnelles pendant lesquelles la totalité de la capacité cible n'est pas entièrement disponible. Bien que le respect des meilleures pratiques Spot en matière de flexibilité en ce qui concerne les types d'instances et les zones de disponibilité offre les meilleures chances d'obtenir une haute disponibilité, rien ne garantit que la capacité sera disponible, car l'augmentation de la demande d'instances à la demande peut perturber les charges de travail sur les instances ponctuelles.

Nous vous déconseillons vivement d'utiliser des instances ponctuelles pour ces charges de travail ou de tenter de passer à des instances à la demande pour gérer les interruptions ou les périodes d'indisponibilité. Le passage à des instances à la demande peut entraîner des interruptions par inadvertance pour vos autres instances ponctuelles. En outre, si les instances ponctuelles correspondant à une combinaison de type d'instance et de zone de disponibilité sont interrompues, il peut s'avérer difficile pour vous d'obtenir des instances à la demande avec cette même combinaison.

Que vous soyez un utilisateur Spot expérimenté ou un nouvel utilisateur des instances Spot, si vous rencontrez actuellement des problèmes avec les interruptions ou la disponibilité des instances Spot, nous vous recommandons de suivre ces bonnes pratiques pour bénéficier de la meilleure expérience d'utilisation du service Spot.

Bonnes pratiques en matière d'instances Spot

- [Préparer des instances individuelles pour les interruptions](#)
- [Soyez flexible en ce qui concerne les types d'instance et les zones de disponibilité](#)
- [Utiliser les groupes Auto Scaling EC2 ou la flotte d'EC2 pour gérer votre capacité agrégée](#)
- [Utiliser la stratégie d'allocation optimisée pour le prix et la capacité](#)
- [Utilisez AWS des services intégrés pour gérer vos instances Spot](#)
- [Quelle est la meilleure méthode de demande Spot à utiliser ?](#)

Préparer des instances individuelles pour les interruptions

La meilleure façon pour vous de gérer fluidement les interruptions d'instance Spot consiste à concevoir votre application pour qu'elle soit tolérante aux pannes. Pour ce faire, vous pouvez tirer parti des recommandations de rééquilibrage d'instance EC2 et des avis d'interruption d'instance Spot.

Le signal de recommandation de rééquilibrage d'instance EC2 vous permet d'être averti lorsqu'une instance Spot présente un risque élevé d'interruption. Le signal vous donne la possibilité de gérer de manière proactive l'instance Spot avant son avis d'interruption à deux minutes. Vous pouvez décider de rééquilibrer votre charge de travail en une instances Spot nouvelle ou existante qui ne présente pas un risque élevé d'interruption. Nous vous avons facilité l'utilisation de ce signal en utilisant la fonctionnalité de rééquilibrage de capacité dans les groupes Auto Scaling et la flotte d'EC2.

Un avis d'interruption d'instance Spot est un avertissement émis deux minutes avant qu'Amazon EC2 l'interrompe. Si votre charge de travail est « flexible dans le temps », vous pouvez configurer vos instances Spot pour qu'elles soient arrêtées ou mises en veille prolongée plutôt que résiliées lorsqu'elles sont interrompues. Amazon EC2 arrête ou met en veille automatiquement vos instances Spot lors de l'interruption et reprend automatiquement les instances lorsque nous disposons de la capacité disponible.

Nous vous recommandons de créer une règle dans [Amazon EventBridge](#) qui capture les recommandations de rééquilibrage et les notifications d'interruption, puis déclenche un point de contrôle pour suivre l'évolution de votre charge de travail ou gère correctement l'interruption. Pour plus d'informations, consultez [Surveiller les signaux de recommandation de rééquilibrage](#). Pour obtenir un exemple détaillé qui vous explique comment créer et utiliser des règles d'événement, consultez [Tirer parti des avis d'interruption d'instance Spot Amazon EC2](#).

Pour plus d'informations, consultez [Recommandations de rééquilibrage des instances EC2 et Interruptions d'instance Spot](#).

Soyez flexible en ce qui concerne les types d'instance et les zones de disponibilité

Un groupe de capacités Spot est un ensemble d'instances EC2 inutilisées avec le même type d'instance (par exemple, `m5.large`) et la même zone de disponibilité (par exemple, `us-east-1a`). Vous devez être flexible quant aux types d'instance que vous demandez et aux zones de disponibilité dans lesquelles vous pouvez déployer votre charge de travail. Cela donne à Spot une meilleure chance de trouver et d'allouer la quantité requise de capacité de calcul. Par exemple, ne demandez pas simplement `c5.large` si vous seriez prêt à utiliser des larges des familles `c4`, `m5` et `m4`.

En fonction de vos besoins spécifiques, vous pouvez évaluer les types d'instance que vous pouvez utiliser pour répondre à vos besoins de calcul. Si une charge de travail peut être mise à l'échelle verticale, vous devez inclure des types d'instance plus importants (plus de vCPU et de mémoire) dans vos requêtes. Si vous ne pouvez évoluer qu'horizontalement, vous devez inclure des types d'instance de génération plus ancienne car ils sont moins demandés par les clients à la demande.

Une bonne règle générale est d'être flexible sur au moins 10 types d'instance pour chaque charge de travail. En outre, assurez-vous que toutes les zones de disponibilité sont configurées pour être utilisées dans votre VPC et sélectionnées pour votre charge de travail.

Utiliser les groupes Auto Scaling EC2 ou la flotte d'EC2 pour gérer votre capacité agrégée

Spot vous permet de penser en termes de capacité agrégée, dans des unités comprenant des vCPUs, de la mémoire, du stockage ou du débit réseau, plutôt que de penser en termes d'instances individuelles. Les groupes Auto Scaling et la flotte d'EC2 vous permettent de lancer et de gérer une capacité cible, et de demander automatiquement des ressources pour remplacer celles qui sont interrompues ou résiliées manuellement. Lorsque vous configurez un groupe Auto Scaling ou une flotte d'EC2, il vous suffit de spécifier les types d'instance et la capacité cible en fonction des besoins de votre application. Pour plus d'informations, consultez la section [Groupes Auto Scaling](#) du Amazon EC2 Auto Scaling Guide de l'utilisateur et la section [Créer une flotte EC2](#) de ce guide de l'utilisateur.

Utiliser la stratégie d'allocation optimisée pour le prix et la capacité

Les stratégies d'allocation dans les groupes Auto Scaling vous aident à provisionner votre capacité cible sans avoir à rechercher manuellement des groupes de capacités Spot avec une capacité de réserve. Nous vous recommandons d'utiliser la stratégie `price-capacity-optimized`, car elle alloue automatiquement les instances des groupes de capacités Spot les plus disponibles qui présentent également le prix le plus bas. Vous pouvez également profiter de la stratégie d'allocation `price-capacity-optimized` dans la flotte d'EC2. Étant donné que votre capacité d'instance Spot provient de pools avec une capacité optimale, cela réduit la possibilité que vos instances Spot soient demandées. Pour plus d'informations sur les stratégies d'allocation, consultez [Instances Spot](#) dans le Amazon EC2 Auto Scaling Guide de l'utilisateur et [Lorsque les charges de travail ont un coût d'interruption élevé](#) dans ce guide de l'utilisateur.

Utilisez AWS des services intégrés pour gérer vos instances Spot

D'autres AWS services s'intègrent à Spot pour réduire les coûts de calcul globaux sans qu'il soit nécessaire de gérer les instances ou les flottes individuelles. Nous vous recommandons d'envisager les solutions suivantes pour vos charges de travail applicables : Amazon EMR, Amazon Elastic Container Service AWS Batch, Amazon Elastic SageMaker Kubernetes Service, Amazon et Amazon.

AWS Elastic Beanstalk GameLift Pour plus d'informations sur les meilleures pratiques Spot avec ces services, consultez le [site Web sur les ateliers Amazon EC2 instances Spot](#).

Quelle est la meilleure méthode de demande Spot à utiliser ?

Utilisez le tableau suivant pour déterminer quelle API utiliser pour les demandes d'instances Spot.

API	Quand l'utiliser ?	Cas d'utilisation	Devrais-je utiliser cette API ?
CreateAutoScalingGroup	<ul style="list-style-type: none"> Vous avez besoin de plusieurs instances avec une configuration unique ou une configuration mixte. Vous voulez automatiser la gestion du cycle de vie via une API configurable. 	Créez un groupe Auto Scaling qui gère le cycle de vie de vos instances tout en gardant le nombre d'instances souhaité. Prend en charge la mise à l'échelle horizontale (ajout d'instances supplémentaires) entre les limites minimale et maximale spécifiées.	Oui
CreateFleet	<ul style="list-style-type: none"> Vous avez besoin de plusieurs instances avec une configuration unique ou une configuration mixte. Vous voulez gérer vous-même le cycle de vie de vos instances. 	Créez une flotte d'instances à la demande et d'instances Spot dans une seule demande, avec plusieurs spécifications de lancement qui varient selon le type d'instance, l'AMI, la zone de disponibilité ou le sous-réseau.	Oui – en mode instant si vous n'avez pas besoin de scalabilité automatique

API	Quand l'utiliser ?	Cas d'utilisation	Devrais-je utiliser cette API ?
	<ul style="list-style-type: none"> • Si vous n'avez pas besoin de scalabilité automatique, nous vous recommandons d'utiliser une flotte de type instant. 	<p>La stratégie d'allocation d'instances Spot est définie par défaut sur <code>lowest-price</code> par unité, mais vous pouvez la modifier en <code>price-capacity-optimized</code>, <code>capacity-optimized</code> ou <code>diversified</code>.</p>	
RunInstances	<ul style="list-style-type: none"> • Vous utilisez déjà l' <code>RunInstances</code> API pour lancer des instances à la demande, et vous souhaitez simplement passer au lancement d'instances Spot en modifiant un seul paramètre. • Vous n'avez pas besoin de plusieurs instances avec des types d'instance différents. 	<p>Lancez un nombre spécifié d'instances en utilisant un AMI et un type d'instance.</p>	<p>Non, car il <code>RunInstances</code> n'autorise pas les types d'instances mixtes dans une seule demande</p>

API	Quand l'utiliser ?	Cas d'utilisation	Devrais-je utiliser cette API ?
RequestSpotFlotte	<ul style="list-style-type: none">• Nous vous déconseillons vivement d'utiliser l' RequestSpotFleet API car il s'agit d'une ancienne API sans investissement prévu.• Si vous souhaitez gérer le cycle de vie de votre instance, utilisez l'CreateFleet API.• Si vous ne souhaitez pas gérer le cycle de vie de votre instance, utilisez l' CreateAutoScalingGroup API.	NE PAS UTILISER. RequestSpotFleet est une ancienne API sans investissement planifié.	Non

API	Quand l'utiliser ?	Cas d'utilisation	Devrais-je utiliser cette API ?
RequestSpotInstances	<ul style="list-style-type: none"> Nous vous déconseillons vivement d'utiliser l' RequestSpotInstances API car il s'agit d'une ancienne API sans investissement prévu. 	NE PAS UTILISER. RequestSpotInstances est une ancienne API sans investissement planifié.	Non

Fonctionnement des instances Spot

Pour lancer une instance Spot, vous devez créer une Demande d'instance Spot, ou qu'Amazon EC2 crée une demande d'instance Spot en votre nom. L'instance Spot se lance lorsque la demande d'instance Spot est remplie.

Vous pouvez lancer une instance Spot en utilisant plusieurs services différents. Pour plus d'informations, consultez [Mise en route avec les instances ponctuelles Amazon EC2](#). Dans ce guide de l'utilisateur, nous décrivons les façons suivantes de lancer une instance Spot à l'aide d'EC2 :

- Vous pouvez créer une demande d'instance Spot à l'aide de l'[assistant de lancement d'instance](#) de la console Amazon EC2 ou de la commande [AWS CLI run-instances](#). Pour plus d'informations, consultez [Créer une demande d'instance Spot](#).
- Vous pouvez créer une flotte EC2 dans laquelle vous spécifiez le nombre souhaité d'instances Spot. Amazon EC2 crée une demande d'instance Spot en votre nom pour chaque instance Spot spécifiée dans la flotte EC2. Pour plus d'informations, consultez [Créer une flotte EC2](#).
- Vous pouvez créer une demande de parc d'instances Spot dans laquelle vous spécifiez le nombre d'instances Spot souhaité. Amazon EC2 crée une demande d'instance Spot en votre nom pour chaque instance Spot spécifiée dans la demande de parc d'instances Spot . Pour plus d'informations, consultez [Créer une Spot Fleet request](#).

Votre instance Spot est lancée si la capacité est disponible.

Votre instance Spot s'exécute jusqu'à ce que vous l'arrêtiez ou la résiliiez, ou jusqu'à ce qu'Amazon EC2 l'interrompe (il s'agit d'une interruption d'instance Spot).

Lorsque vous utilisez des instances Spot, vous devez être prêt à des interruptions. Amazon EC2 peut interrompre votre instance Spot lorsque la demande d'instances Spot augmente ou lorsque l'offre d'instances Spot diminue. Lorsqu'Amazon EC2 interrompt une instance Spot, il communique un avis d'interruption d'instance Spot, ce qui avertit l'instance qu'Amazon EC2 va l'interrompre dans deux minutes. Vous ne pouvez pas activer la protection de la résiliation pour les instances Spot. Pour plus d'informations, consultez [Interruptions d'instance Spot](#).

Vous pouvez arrêter, démarrer, redémarrer ou résilier une instance Spot basée sur Amazon EBS. Le service Spot peut arrêter, résilier ou mettre en veille prolongée une instance Spot lorsqu'il l'interrompt.

Sommaire

- [Lancer une instances Spot dans un groupe de lancement](#)
- [Lancer une instances Spot dans un groupe de zone de disponibilité](#)
- [Lancer une instances Spot dans un VPC](#)

Lancer une instances Spot dans un groupe de lancement

Spécifiez un groupe de lancement dans votre demande d'instance Spot pour demander à Amazon EC2 de lancer un ensemble d'instances Spot uniquement s'il peut toutes les lancer. De plus, si le service Spot doit résilier l'une des instances du groupe de lancement, il doit toutes les résilier. Toutefois, si vous mettez hors service une ou plusieurs instances d'un groupe de lancement, Amazon EC2 ne met pas hors service les instances restantes du groupe de lancement.

Même si cette option peut être utile, l'ajout d'une contrainte de ce type peut réduire les chances de voir votre demande d'instance Spot satisfaite et accroître les risques de suppression de vos instances Spot. Par exemple, votre groupe de lancement inclut des instances figurant dans plusieurs zones de disponibilité. Si la capacité dans l'une de ces zones de disponibilité diminue et n'est plus disponible, Amazon EC2 résilie alors toutes les instances du groupe de lancement.

Si vous créez une autre demande d'instance Spot réussie qui spécifie le même groupe de lancement (existant) qu'une demande précédente réussie, les nouvelles instances sont ajoutées au groupe de lancement. Par conséquent, si une instance de ce groupe de lancement est mise hors service, toutes les instances du groupe de lancement sont également mises hors service, ce qui inclut les instances lancées par les première et deuxième demandes.

Lancer une instances Spot dans un groupe de zone de disponibilité

Spécifiez un groupe de zone de disponibilité dans votre demande d'instance Spot pour dire à Amazon EC2 de lancer un ensemble d'instances Spot dans la même zone de disponibilité. Amazon EC2 n'a pas besoin d'interrompre toutes les instances d'un groupe de zone de disponibilité en même temps. Si Amazon EC2 doit interrompre l'une des instances d'un groupe de zone de disponibilité, les autres continuent à être exécutées.

Même si cette option peut s'avérer utile, l'ajout d'une contrainte de ce type peut réduire les chances de voir votre demande d'instance Spot satisfaite.

Si vous spécifiez un groupe de zone de disponibilité, mais que vous n'indiquez aucune zone de disponibilité dans la demande d'instance Spot, le résultat dépend du réseau que vous avez spécifié.

VPC par défaut

Amazon EC2 utilise la zone de disponibilité pour le sous-réseau spécifié. Si vous ne spécifiez pas de sous-réseau, le service sélectionne une zone de disponibilité et son sous-réseau par défaut, mais pas nécessairement la zone ayant le prix le plus bas. Si vous avez supprimé le sous-réseau par défaut pour une zone de disponibilité, vous devez spécifier un autre sous-réseau.

VPC personnalisé

Amazon EC2 utilise la zone de disponibilité pour le sous-réseau spécifié.

Lancer une instances Spot dans un VPC

Vous spécifiez un sous-réseau pour vos instances Spot de la même façon que vous spécifiez un sous-réseau pour vos instances à la demande.

- [VPC par défaut] Si vous souhaitez que votre instance Spot soit lancée dans une zone de disponibilité à faible prix, vous devez spécifier le sous-réseau correspondant dans votre demande d'instance Spot. Si vous ne spécifiez pas de sous-réseau, Amazon EC2 en sélectionne un pour vous et la zone de disponibilité de ce sous-réseau ne correspondra peut-être pas au prix Spot le plus faible.
- [VPC personnalisé] Vous devez spécifier le sous-réseau de votre instance Spot.

Historique de tarification d'instances Spot

Les prix d'instance Spot sont définis par Amazon EC2 et ajustés graduellement en fonction des tendances à long terme en matière d'offre et de demande de capacité d'instance Spot.

Lorsque votre demande d'instance Spot est satisfaite, vos instances Spot se lancent au prix Spot actuel, sans dépasser le prix à la demande. Vous pouvez consulter l'historique des prix Spot pour les 90 derniers jours en filtrant par type d'instance, système d'exploitation et zone de disponibilité.

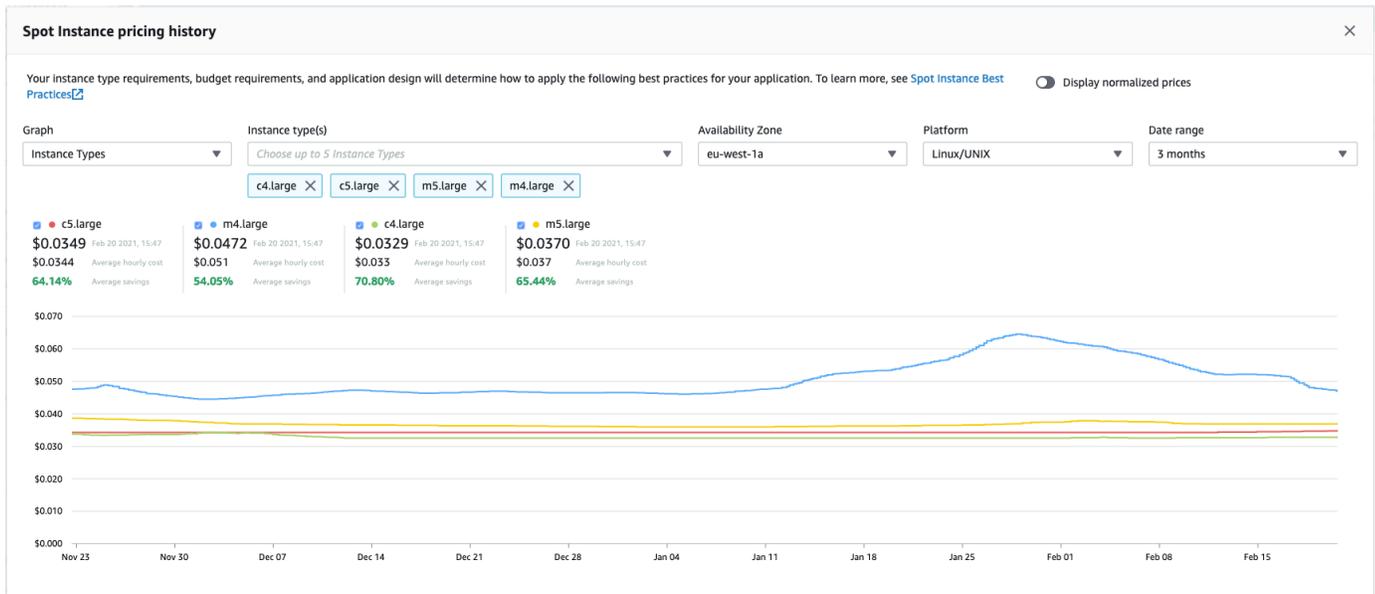
Pour afficher les prix Spot actuels

Pour connaître les prix actuels des instances Spot, consultez la [Tarification des instances Spot Amazon EC2](#).

Pour consulter l'historique des prix au comptant à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez Historique de tarification.
4. Pour Graph (Graphique), choisissez de comparer l'historique des prix par Availability Zones (Zones de disponibilité) ou par Instance Types (Types d'instance).
 - Si vous choisissez Availability Zones (Zones de disponibilité), alors sélectionnez le Instance type (Type d'instance), le système d'exploitation (Platform (Plateforme)) et la Date range (Plage de dates) pour lesquels afficher l'historique des prix.
 - Si vous sélectionnez Instance Types (Types d'instance), alors choisissez jusqu'à 5 Instance type(s) (Type(s) d'instance), la Availability Zone (Zone de disponibilité), le système d'exploitation (Platform (Plateforme)) et la Date range (Plage de dates) pour lesquels afficher l'historique des prix.

La capture d'écran suivante présente une comparaison de prix pour différents types d'instance.



5. Survolez le graphique avec le pointeur de la souris pour afficher les prix à des moments donnés dans la plage de dates sélectionnée. Les prix sont affichés dans les blocs d'informations au-dessus du graphique. Le prix affiché dans la ligne supérieure indique le prix à une date spécifique. Le prix affiché sur la deuxième ligne indique le prix moyen sur la plage de dates sélectionnée.
6. Pour afficher le prix par vCPU, basculez sur Display normalized prices (Afficher les prix normalisés). Pour afficher le prix du type d'instance, désactivez Display normalized prices (Afficher les prix normalisés).

Pour afficher l'historique des prix Spot à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations, consultez [Accès à Amazon EC2](#).

- [describe-Spot-price-history](#) (AWS CLI)
- [Get-EC2SpotPriceHistory](#) (AWS Tools for Windows PowerShell)

Économies réalisées grâce à l'achat d'instances Spot

Vous pouvez visualiser les informations relatives à l'utilisation et aux économies réalisées grâce aux instances Spot pour chaque flotte ou pour l'ensemble des instances Spot en cours d'exécution. Les informations relatives à l'utilisation et aux économies pour chaque flotte incluent l'ensemble des

instances lancées et résiliées par la flotte. Ces informations peuvent être consultées pour la dernière heure ou pour les trois derniers jours.

La capture d'écran suivante de la section Economie illustre les informations relatives à l'utilisation d'instances Spot et aux économies associées pour un parc d'instances Spot.

Spot usage and savings

4	266	700	\$9.55	\$2.99	69%
Spot Instances	vCPU-hours	Mem(GiB)-hours	On-Demand total	Spot total	Savings
				\$0.0112	\$0.0043
				Average cost per VCPU-hour	Average cost per mem(GiB)-hour

Details

Instance type	vCPU hours	Mem(GiB)-hours	On-Demand total	Spot total	Savings
t3.medium (1)	2 vCPU hours	4 mem(GiB)-hours	\$0.01 total	\$0.01 total	70% savings
m4.large (1)	144 vCPU hours	576 mem(GiB)-hours	\$2.52 total	\$2.52 total	68% savings
t2.micro (2)	120 vCPU hours	120 mem(GiB)-hours	\$0.46 total	\$0.46 total	70% savings

Les informations suivantes relatives à l'utilisation et aux économies sont disponibles :

- Instances Spot – Nombre d'instances. Spot lancées et terminées par le parc d'instances Spot. Le nombre qui apparaît dans le récapitulatif des économies représente l'ensemble de vos instances Spot en cours d'exécution.
- vCPU-hours (Heures vCPU) : nombre d'heures vCPU utilisées pour l'ensemble des Instances Spot sur la période sélectionnée.
- Mem(GiB)-hours (Heures de mémoire (Gio)) : nombre d'heures Gio utilisées pour l'ensemble des Instances Spot sur la période sélectionnée.
- On-Demand total (Total à la demande) : montant total que vous auriez payé pour la période sélectionnée si vous aviez lancé ces instances en tant qu'Instances à la demande.
- Spot total (Total Spot) : montant total à payer pour la période sélectionnée.
- Économie : pourcentage que vous économisez en ne payant pas le prix à la demande.

- Average cost per vCPU-hour (Coût moyen par heure vCPU) : coût horaire moyen de l'utilisation des vCPU pour l'ensemble des Instances Spot sur la période sélectionnée, calculé comme suit :
Coût moyen par heure vCPU = Total Spot / Heures vCPU.
- Coût moyen par mém (GiB) par heure — Le coût horaire moyen de l'utilisation de toutes GiBs les instances ponctuelles pendant la période sélectionnée, calculé comme suit : coût moyen par mém (GiB) -heure = total spot/Mem (GiB) -heures.
- Tableau Détails – Les différents types d'instances (le nombre d'instances par type d'instance est placé entre parenthèses) qui composent le parc d'instances Spot. Le récapitulatif des économies comprend l'ensemble de vos instances Spot en cours d'exécution.

Vous ne pouvez consulter les informations relatives aux économies qu'à l'aide de la console Amazon EC2.

Pour consulter les informations relatives aux économies réalisées sur un parc Spot à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez l'ID d'une demande de parc d'instances Spot et faites défiler jusqu'à la section Economie.

Vous pouvez également cocher la case en regard de l'ID de demande de parc d'instances Spot, puis choisir l'onglet Economie.

4. Par défaut, la page affiche les informations relatives à l'utilisation et aux économies de ces trois derniers jours. Vous pouvez choisir last hour (dernière heure) ou last three days (trois derniers jours). Pour les Parcs d'instances Spot qui ont été lancés il y a moins d'une heure, la page affiche une estimation des économies réalisées sur cette heure.

Pour consulter les informations relatives aux économies réalisées pour toutes les instances Spot en cours d'exécution à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Choisissez Savings Summary (Récapitulatif des économies).

Utiliser instances Spot

Pour utiliser des instances Spot, vous créez une demande d'instance Spot qui inclut le nombre d'instances souhaité, le type d'instance et la zone de disponibilité. Si la capacité est disponible, Amazon EC2 répond à votre demande immédiatement. Dans le cas contraire, Amazon EC2 attend jusqu'à ce que votre demande soit exécutée ou jusqu'à l'annulation de celle-ci.

L'illustration suivante présente le fonctionnement des demandes d'instances Spot. Notez que le type de demande (unique ou persistante) détermine si la demande est rouverte lorsqu'Amazon EC2 interrompt une instance Spot ou que vous arrêtez une instance Spot. Si la demande est persistante, elle est rouverte après que votre instance Spot soit interrompue. Si la demande est persistante et que vous arrêtez votre instance Spot, la demande s'ouvre seulement après que vous ayez démarré votre instance Spot.

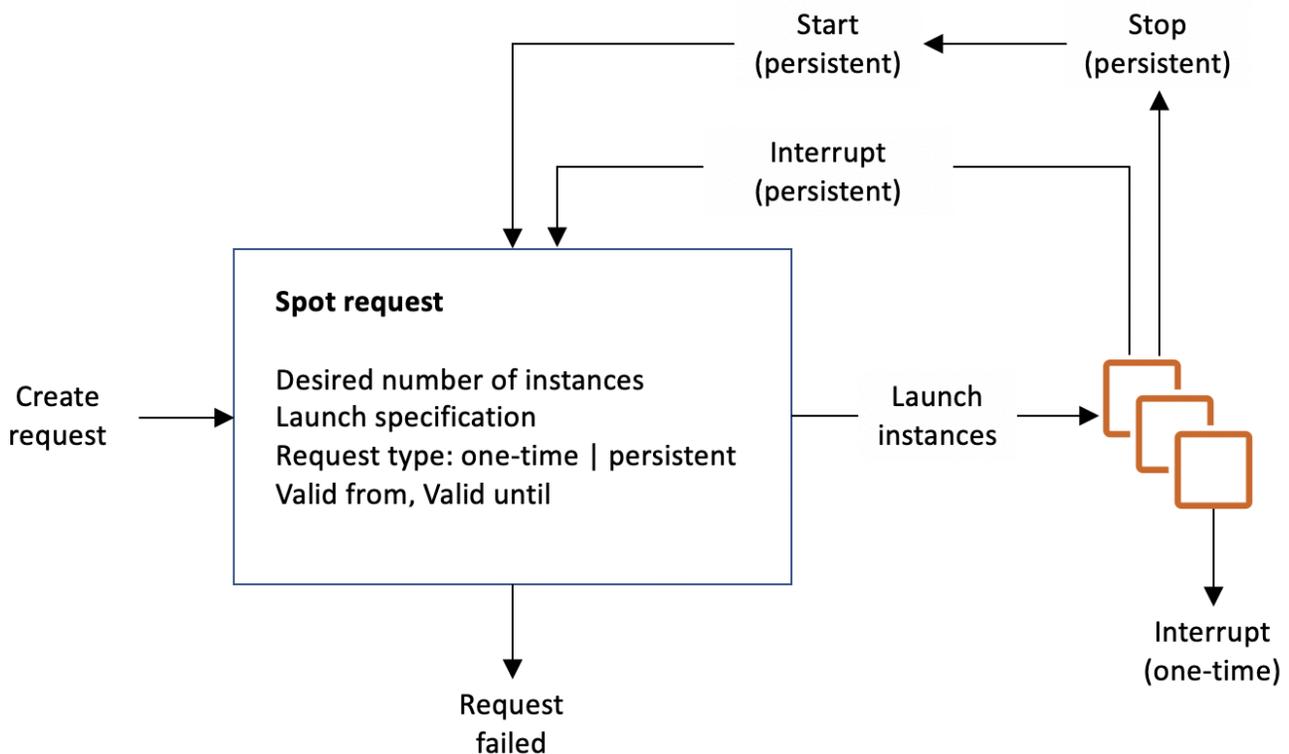


Table des matières

- [États des demandes d'instance Spot](#)
- [Spécifier une location pour votre instances Spot](#)
- [Rôle lié à un service pour les demandes d'instance Spot](#)

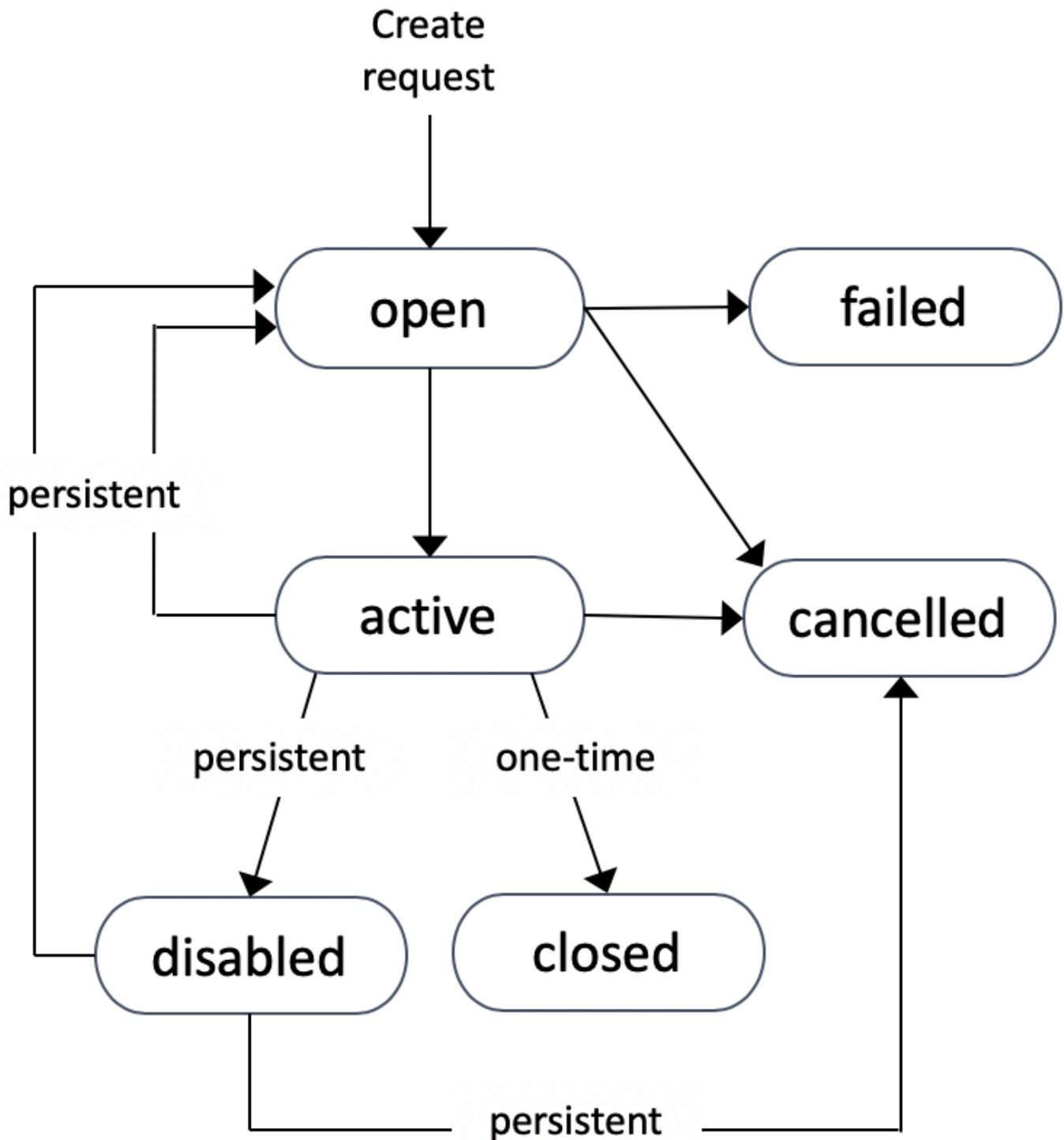
- [Créer une demande d'instance Spot](#)
- [Trouvez vos instances Spot](#)
- [Marquer les demandes d'instance Spot](#)
- [Annuler une demande d'instance Spot](#)
- [Arrêt d'une instance Spot](#)
- [Démarrer une instance Spot](#)
- [Résilier une instance Spot](#)
- [Exemple de spécifications de lancement d'une demande d'instance Spot](#)

États des demandes d'instance Spot

Une demande d'instance Spot peut avoir l'un des états suivants :

- `open` – La demande est en attente d'exécution.
- `active` – La demande a été exécutée et est associée à une instance Spot.
- `failed` – La demande a un ou plusieurs paramètres erronés.
- `closed` – L'instance Spot a été interrompue ou résiliée.
- `disabled` – Vous avez arrêté l'instance Spot.
- `cancelled` – Vous avez annulé la demande ou elle est arrivée à expiration.

L'illustration suivante représente les transitions entre les états de la demande. Remarquez que les transitions dépendent du type de demande (unique ou persistante).



Une demande d'instance Spot unique reste active jusqu'à ce qu'Amazon EC2 lance l'instance Spot, que la demande arrive à expiration ou que vous annuliez la demande. Si la capacité n'est pas disponible, votre instance Spot est résiliée et la demande d'instance Spot est close.

Une demande d'instance Spot persistante reste active jusqu'à ce qu'elle arrive à expiration ou que vous l'annuliez, même si la demande est satisfaite. Si la capacité n'est pas disponible, votre instance Spot est interrompue. Une fois que votre instance a été interrompue, lorsque la capacité redevient disponible, l'instance Spot est démarrée si elle a été arrêtée, ou reprise si elle a été mise en veille prolongée. Vous pouvez arrêter une instance Spot et la redémarrer si la capacité est disponible. Si l'instance Spot est résiliée (que l'instance Spot soit à l'état arrêté ou en cours d'exécution), la demande d'instance Spot est rouverte et Amazon EC2 lance une nouvelle instance Spot. Pour plus d'informations, consultez [Arrêt d'une instance Spot](#), [Démarrer une instance Spot](#) et [Résilier une instance Spot](#).

Vous pouvez effectuer le suivi du statut de vos demandes d'instance Spot, ainsi que celui des instances Spot lancées, via le statut. Pour plus d'informations, consultez [Statut des demandes Spot](#).

Spécifier une location pour votre instances Spot

Vous pouvez exécuter une instance Spot sur du matériel à client unique. Les instances Spot dédiées sont physiquement isolées des instances appartenant à d'autres AWS comptes. Pour plus d'informations, consultez [Dedicated instances](#) et la page produit [Instances dédiées Amazon EC2](#).

Pour exécuter une instance Spot dédiée, effectuez l'une des actions suivantes :

- Spécifiez une location de `dedicated` au moment de créer la demande d'instance Spot. Pour plus d'informations, consultez [Créer une demande d'instance Spot](#).
- Demandez une instance Spot sur un VPC avec une location d'instance de `dedicated`. Pour plus d'informations, consultez [Créer un VPC avec une location d'instance dédiée](#). Vous ne pouvez pas demander d'instance Spot avec une location de `default` si vous la demandez sur un VPC avec une location d'instance de `dedicated`.

Toutes les familles d'instances prennent en charge les instances Spot dédiées sauf les instances T. Pour chaque famille d'instances prise en charge, seule la plus grande taille d'instance ou taille de métal prend en charge les instances Spot dédiées.

Rôle lié à un service pour les demandes d'instance Spot

Amazon EC2 utilise des rôles liés à un service pour les autorisations requises pour appeler d'autres services AWS en votre nom. Un rôle lié à un service est un type unique de rôle IAM directement lié à un service. AWS Les rôles liés à un service constituent un moyen sécurisé de déléguer des autorisations aux AWS services, car seul le service lié peut assumer un rôle lié au service. Pour plus d'informations, consultez [Utilisation des rôles liés à un service](#) dans le IAM Guide de l'utilisateur.

Amazon EC2 utilise le rôle lié au service nommé `AWSServiceRoleForEC2Spot` pour lancer et gérer les instances Spot en votre nom.

Autorisations octroyées par `AWSServiceRoleForEC2Spot`

Amazon EC2 permet `AWSServiceRoleForEC2Spot` d'effectuer les actions suivantes :

- `ec2:DescribeInstances` – Décrire les instances Spot
- `ec2:StopInstances` – Arrêter les instances Spot
- `ec2:StartInstances` – Démarrer les instances Spot

Création du rôle lié à un service

Dans la plupart des cas, vous n'avez pas besoin de créer manuellement un rôle lié à un service. Amazon EC2 crée le rôle `AWSServiceRoleForEC2Spot` lié au service la première fois que vous demandez une instance Spot à l'aide de la console.

Si vous avez reçu une demande d'instance Spot active avant octobre 2017, date à laquelle Amazon EC2 a commencé à prendre en charge ce rôle lié à un service, Amazon EC2 a créé le rôle dans votre compte. `AWSServiceRoleForEC2Spot` AWS Pour plus d'informations, consultez [Un nouveau rôle est apparu dans mon compte](#) dans le IAM Guide de l'utilisateur.

Si vous utilisez l'API AWS CLI ou une API pour demander une instance Spot, vous devez d'abord vous assurer que ce rôle existe.

Pour créer `AWSServiceRoleForEC2Spot` à l'aide de la console

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Rôles.
3. Sélectionnez Créer un rôle.
4. Sur la page Select type of trusted entity (Sélectionner le type d'entité de confiance), choisissez EC2, EC2 - Spot Instances (EC2 - Instances Spot), Suivant : Autorisations.
5. Sur la page suivante, choisissez Suivant : Vérification.
6. Sur la page Vérification, choisissez Create Role (Créer un rôle).

Pour créer à `AWSServiceRoleForEC2Spot` l'aide du AWS CLI

Utilisez la commande [create-service-linked-role](#) comme suit.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Si vous n'avez plus besoin d'utiliser des instances Spot, nous vous recommandons de supprimer le AWSServiceRoleForEC2Spotrôle. Une fois ce rôle supprimé de votre compte, Amazon EC2 crée de nouveau le rôle si vous effectuez une demande d'instances Spot.

Octroyer un accès aux clés gérées par le client (CMK) en vue de leur utilisation avec les AMI chiffrées et les instantanés EBS

Si vous spécifiez une [AMI chiffrée](#) ou un instantané Amazon EBS chiffré pour vos instances Spot et que vous utilisez une clé gérée par le client pour le chiffrement, vous devez accorder au AWSServiceRoleForEC2Spotrôle l'autorisation d'utiliser la clé gérée par le client afin qu'Amazon EC2 puisse lancer des instances Spot en votre nom. Pour cela, vous devez ajouter une autorisation à la clé gérée par le client, comme indiqué dans la procédure suivante.

Lorsque vous définissez les autorisations, les octrois constituent une alternative aux politiques de clé. Pour de plus amples informations, veuillez consulter [Utilisation des octrois](#) et [Utilisation des stratégies de clé dans AWS KMS](#) dans le Guide du développeur AWS Key Management Service .

Pour autoriser le rôle AWSServiceRoleForEC2Spot à utiliser la clé gérée par le client

- Utilisez la commande [create-grant](#) pour ajouter une autorisation à la clé gérée par le client et pour spécifier le principal (le rôle AWSServiceRoleForEC2Spotlié au service) autorisé à effectuer les opérations autorisées par l'autorisation. La clé gérée par le client est spécifiée par le paramètre `key-id` et l'ARN de la clé gérée par le client. Le principal est spécifié par le `grantee-principal` paramètre et l'ARN du rôle AWSServiceRoleForEC2Spotlié au service.

```
aws kms create-grant \  
  --region us-east-1 \  
  --key-id arn:aws:kms:us-  
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \  
  --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/  
spot.amazonaws.com/AWSServiceRoleForEC2Spot \  
  --operations "Decrypt" "Encrypt" "GenerateDataKey"  
"GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"  
"ReEncryptTo"
```

Créer une demande d'instance Spot

Vous pouvez utiliser l'[assistant de lancement d'instance](#) de la console Amazon EC2 ou la AWS CLI commande [run-instances](#) pour demander une instance Spot de la même manière que vous pouvez lancer une instance à la demande. Cette méthode n'est recommandée que pour les raisons suivantes :

- Vous utilisez déjà l'[assistant de lancement d'instance](#) ou la commande [run-instances](#) pour lancer des instances à la demande, et vous voulez simplement passer au lancement d'instances Spot en modifiant un seul paramètre.
- Vous n'avez pas besoin de plusieurs instances avec des types d'instance différents.

Cette méthode n'est généralement pas recommandée pour le lancement d'instances Spot car vous ne pouvez pas spécifier plusieurs types d'instance et vous ne pouvez pas lancer d'instances Spot et d'instances à la demande dans la même requête. Pour connaître les méthodes préférées pour lancer des instances Spot, notamment le lancement d'une flotte qui inclut des instances Spot et des instances à la demande avec plusieurs types d'instance, veuillez consulter la rubrique [Quelle est la meilleure méthode de demande Spot à utiliser ?](#)

Si vous demandez plusieurs instances Spot à la fois, Amazon EC2 crée des demandes d'instance Spot distinctes pour vous permettre de suivre l'état de chaque demande séparément. Pour plus d'informations sur le suivi des demandes d'instance Spot, consultez [Statut des demandes Spot](#).

New console

Pour créer une demande d'Instance Spot à l'aide de l'assistant de lancement d'instance

Les étapes 1 à 9 sont les mêmes que celles que vous utiliseriez pour lancer une instance à la demande. À l'étape 10, vous configurez la demande d'instance Spot.

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, en haut de l'écran, sélectionnez une région.
3. Sur le tableau de bord de la console Amazon EC2, sélectionnez Launch instance (Lancer une instance).
4. (Facultatif) Sous Name and tags (Noms et identifications), vous pouvez nommer votre instance et étiqueter la demande d'instance Spot, l'instance, les volumes et les Elastic Graphics. Pour plus d'informations sur les balises, consultez [Baliser vos ressources Amazon EC2](#).

- a. Pour Name (Nom), saisissez un nom descriptif pour votre instance.

Le nom de l'instance est une identification, où la clé est Name (Nom), et la valeur est le nom que vous spécifiez. Si vous ne spécifiez pas de nom, l'instance peut être identifiée par son ID, qui est automatiquement généré lorsque vous lancez l'instance.

- b. Pour étiqueter la demande d'instance Spot, l'instance, les volumes et les Elastic Graphics, choisissez Add additional tags (Ajouter de identifications supplémentaires). Choisissez Add tag (Ajouter une identification), saisissez une clé et une valeur, puis sélectionnez le type de ressource à étiqueter. Choisissez Add tag (Ajouter une identification) pour chaque étiquette supplémentaire.

5. Sous Application and OS Images (Amazon machine Image) (Images d'applications et de systèmes d'exploitation [Amazon machine Image]), choisissez le système d'exploitation de votre instance, puis sélectionnez une AMI. Pour plus d'informations, consultez [Images d'applications et de systèmes d'exploitation \(Amazon Machine Image\)](#).
6. Sous Instance type (Type d'instance), sélectionnez le type d'instance qui répond à vos exigences en ce qui concerne la configuration matérielle et la taille de votre instance. Pour plus d'informations, consultez [Type d'instance](#).
7. Sous Key pair (login) (Paire de clés [connexion]), choisissez une paire de clés existante ou choisissez Create new key pair (Créer une paire de clés) pour en créer une. Pour plus d'informations, consultez [Paires de clés Amazon EC2 et instances Amazon EC2](#).

 Important

Si vous sélectionnez l'option Proceed without key pair (Not recommended) ((Continuer sans paire de clé) (Non recommandé)), vous ne pourrez pas vous connecter à l'instance à moins de choisir une AMI configurée de façon à autoriser les utilisateurs à se connecter d'une autre façon.

8. Sous Network settings (Paramètres réseau), utilisez les paramètres par défaut ou choisissez Edit (Modifier) pour configurer les paramètres réseau selon les besoins.

Les groupes de sécurité font partie des paramètres réseau et définissent les règles de pare-feu pour votre instance. Ces règles déterminent le trafic réseau entrant acheminé vers votre instance.

Pour plus d'informations, consultez [Paramètres réseau](#).

9. L'AMI sélectionnée inclut un ou plusieurs volumes de stockage, notamment le volume du périphérique racine. Sous Configure storage (Configurer le stockage), vous pouvez spécifier des volumes supplémentaires à attacher à l'instance en choisissant Add new volume (Ajouter un nouveau volume). Pour plus d'informations, consultez [Configurer le stockage](#).
10. Sous Advanced details (Détails avancés), configurez la demande d'instance Spot comme suit :
 - a. Sous Purchasing option (Option d'achat), cochez la case Request Spot Instances (Demander des instances Spot).
 - b. Vous pouvez soit conserver la configuration par défaut de la demande d'instance Spot, soit choisir Customize (Personnaliser), à droite, pour spécifier des paramètres personnalisés pour votre demande d'instance Spot.

Lorsque vous choisissez Customize (Personnaliser), les champs suivants s'affichent.

- i. Maximum price (Prix maximal) : vous pouvez demander des instances Spot au prix Spot, plafonné au prix À la demande, ou spécifier le montant maximum que vous êtes prêt à payer.

 Warning

Si vous spécifiez un prix maximum, vos instances seront interrompues plus fréquemment que si vous choisissez No maximum price (Pas de prix maximal).

- No maximum price (Pas de prix maximal) : votre instance Spot sera lancée au prix Spot en vigueur. Le prix ne dépassera jamais le prix À la demande. (Recommandé)
- Set your maximum price (per instance/hour) (Définir votre prix maximal, par instance/heure) : vous pouvez spécifier le montant maximum que vous êtes prêt à payer.
 - Si vous spécifiez un prix maximum inférieur au prix Spot, votre instance Spot n'est pas lancée.
 - Si vous spécifiez un prix maximum supérieur au prix Spot actuel, votre Instance Spot sera lancée et facturée au prix Spot actuel. Une fois que votre instance

Spot est en cours d'exécution, si le prix Spot dépasse votre prix maximum, Amazon EC2 interrompt votre instance Spot.

- Quel que soit le prix maximum que vous spécifiez, vous serez toujours facturé au prix Spot actuel.

Pour passer en revue les tendances de prix Spot, consultez [Historique de tarification d'instances Spot](#).

- ii. Request type (Type de demande) : le type de demande d'instance spot que vous choisissez détermine ce qui se passe si votre instance spot est interrompue.
 - One-time (Unique) : Amazon EC2 effectue une demande unique pour votre instance Spot. Si votre instance Spot est interrompue, la demande n'est pas soumise à nouveau.
 - Persistent request (Demande persistante) : Amazon EC2 place une demande persistante pour votre instance Spot. Si votre instance spot est interrompue, la demande est soumise à nouveau afin de réapprovisionner l'instance spot résiliée.

Si vous ne spécifiez pas de valeur, la valeur par défaut est une demande unique.

- iii. Valid to (Valable jusqu'au) : date d'expiration d'une demande persistante d'instance Spot.

Ce champ n'est pas pris en charge pour les demandes uniques. Une demande d'unique reste active jusqu'à ce que toutes les instances de la demande soient lancées ou que vous annuliez la demande.

- No request expiry date (Pas de date d'expiration de la demande) : la demande reste active jusqu'à ce que vous l'annuliez.
 - Set your request expiry date (Définir la date d'expiration de votre demande) : la demande persistante reste active jusqu'à la date spécifiée ou jusqu'à ce que vous l'annuliez.
- iv. Interruption behavior (Comportement d'interruption) : le comportement que vous choisissez détermine ce qui se passe lorsqu'une instance spot est interrompue.
 - Pour les demandes persistantes, les valeurs valides sont Stop (Arrêter) et Hibernate (Mettre en veille prolongée). Lorsqu'une instance est arrêtée, des frais pour le stockage de volume EBS s'appliquent.

Note

Les instances Spot utilisent désormais la même fonctionnalité de mise en veille prolongée que les instances à la demande. Pour activer la mise en veille prolongée, vous pouvez soit choisir Mise en veille prolongée ici, soit sélectionner Activer dans le champ Comportement d'arrêt – mise en veille prolongée, qui apparaît plus bas dans l'assistant de lancement d'instance. Pour les prérequis de mise en veille prolongée, consultez [Conditions préalables à l'hibernation des instances Amazon EC2](#).

- Pour les demandes uniques, seule la valeur Terminate (Résilier) est valide.

Si vous ne spécifiez pas de valeur, la valeur par défaut est Terminate (Résilier), laquelle n'est pas valide pour une demande d'instance Spot persistante. Si vous conservez la valeur par défaut et tentez de lancer une demande d'instance Spot persistante, une erreur s'affiche.

Pour plus d'informations, consultez [Comportement des interruptions des instances Spot](#).

11. Sur le panneau Summary (Récapitulatif), pour Number of instances (Nombre d'instances), saisissez le nombre d'instances à lancer.

Note

Amazon EC2 crée une demande distincte pour chaque instance Spot.

12. Sur le panneau Summary (Récapitulatif), vérifiez les détails de votre instance et effectuez toute modification nécessaire. Après avoir soumis votre demande d'instance Spot, vous ne pouvez plus modifier les paramètres de la demande. Vous pouvez accéder directement à une section dans l'assistant de lancement d'instance en sélectionnant son lien dans le panneau Summary (Récapitulatif). Pour plus d'informations, consultez [Récapitulatif](#).
13. Lorsque vous êtes prêt à lancer votre instance, choisissez Launch instance (Lancer l'instance).

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à terminated au lieu de running, consultez [Résoudre les problèmes de lancement d'instance](#).

Old console

Pour créer une demande d'Instance Spot à l'aide de l'assistant de lancement d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, en haut de l'écran, sélectionnez une région.
3. Sur le tableau de bord de la console Amazon EC2, sélectionnez Lancer une instance.
4. Sur la page Sélection d'une Amazon Machine Image (AMI), choisissez une AMI de la façon suivante : Pour plus d'informations, consultez [Étape 1 : Sélectionner d'une Amazon Machine Image \(AMI\)](#).
5. Sur la page Choose an Instance Type (Choisir un type d'instance), sélectionnez la configuration matérielle et la taille de l'instance à lancer, puis choisissez Next: Configure Instance Details (Suivant : Configurer les détails de l'instance). Pour plus d'informations, consultez [Étape 2 : Choisir un type d'instance](#).
6. Sur la page Configurer les détails de l'instance, configurez la demande d'instance Spot comme suit :
 - Nombre d'instances : entrez le nombre d'instances à lancer.

Note

Amazon EC2 crée une demande distincte pour chaque instance Spot.

- (Facultatif) Afin d'avoir un nombre suffisant d'instances pour gérer la demande sur votre application, vous pouvez choisir Lancer dans un groupe Auto Scaling pour créer une configuration de lancement et un groupe Auto Scaling. La fonctionnalité Auto Scaling fait évoluer le nombre d'instances du groupe en fonction de vos spécifications. Pour plus d'informations, consultez le [Guide de l'utilisateur Amazon EC2 Auto Scaling](#).
- Option d'achat : sélectionnez Demander des instances Spot pour lancer une instance Spot. Lorsque vous choisissez cette option, les champs suivants s'affichent.
- Prix actuel : le prix Spot actuel dans chaque zone de disponibilité s'affiche pour le type d'instance sélectionné.
- (Facultatif) Prix maximum : vous pouvez laisser le champ vide ou spécifier le montant maximum que vous êtes prêt à payer.

⚠ Warning

Si vous spécifiez un prix maximum, vos instances seront interrompues plus fréquemment que si vous laissez le champ vide.

- Si vous spécifiez un prix maximum inférieur au prix Spot, votre Instance Spot ne sera pas lancée.
- Si vous spécifiez un prix maximum supérieur au prix Spot actuel, votre Instance Spot sera lancée et facturée au prix Spot actuel. Une fois que votre instance Spot est en cours d'exécution, si le prix Spot dépasse votre prix maximum, Amazon EC2 interrompt votre instance Spot.
- Quel que soit le prix maximum que vous spécifiez, vous serez toujours facturé au prix Spot actuel.
- Si vous laissez le champ vide, vous paierez le prix Spot actuel.
- Demande persistante : choisissez Demande persistante pour soumettre à nouveau la demande d'instance Spot si votre instance Spot est interrompue.
- Comportement d'interruption : par défaut, le service Spot résilie une instance Spot lorsqu'elle est interrompue. Si vous choisissez Demande persistante, vous pouvez alors spécifier que le service Spot arrête votre instance Spot ou la mette en veille prolongée lorsqu'elle est interrompue. Pour plus d'informations, consultez [Comportement des interruptions des instances Spot](#).
- (Facultatif) Demande valide pour : choisissez Modifier pour spécifier l'expiration de la demande d'instance Spot.

Pour plus d'informations sur la configuration de votre instance Spot, consultez [Étape 3 : Configurer les détails de l'instance](#).

7. L'AMI sélectionnée inclut un ou plusieurs volumes de stockage, notamment le volume du périphérique racine. Sur la page Ajouter le stockage, vous pouvez spécifier des volumes supplémentaires à attacher à l'instance en choisissant Ajouter un nouveau volume. Pour plus d'informations, consultez [Étape 4 : Ajouter du stockage](#).
8. Sur la page Ajouter des balises, spécifiez les [balises](#) en fournissant les combinaisons clé et valeur. Pour plus d'informations, consultez [Étape 5 : Ajouter des balises](#).

9. Sur la page Configurer le groupe de sécurité, utilisez un groupe de sécurité afin de définir les règles de pare-feu de votre instance. Ces règles déterminent le trafic réseau entrant acheminé vers votre instance. Le reste du trafic est ignoré. (Pour plus d'informations sur les groupes de sécurité, consultez [Groupes de sécurité Amazon EC2 pour vos instances EC2.](#)) Sélectionnez ou créez un groupe de sécurité de la façon suivante, puis choisissez Vérifier et lancer. Pour plus d'informations, consultez [Étape 6 : Configurer un groupe de sécurité.](#)
10. Sur la page Examiner le lancement de l'instance, vérifiez les détails de votre instance, puis effectuez les modifications nécessaires en sélectionnant le lien Modifier approprié. Une fois que vous êtes prêt, choisissez Lancer. Pour plus d'informations, consultez [Étape 7 : Vérifier le lancement de l'instance et sélectionner une paire de clés.](#)
11. Dans la boîte de dialogue Select an existing key pair or create a new key pair (Sélectionner une paire de clés existante ou créer une nouvelle paire de clés), vous pouvez choisir une paire de clés existante ou en créer une nouvelle. Par exemple, sélectionnez Choisir une paire de clés existante, puis choisissez la paire de clés que vous avez créée lors de la configuration. Pour plus d'informations, consultez [Paires de clés Amazon EC2 et instances Amazon EC2.](#)

 Important

Si vous sélectionnez l'option Proceed without key pair (Continuer sans paire de clé), vous ne pourrez pas vous connecter à l'instance à moins de choisir une AMI configurée de façon à autoriser les utilisateurs à se connecter d'une autre façon.

12. Pour lancer votre instance, activez la case à cocher de confirmation, puis choisissez Lancer des instances.

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez [Résoudre les problèmes de lancement d'instance.](#)

AWS CLI

Pour créer une demande d'instance Spot à l'aide de [run-instances](#)

Utilisez la commande [run-instances](#) et spécifiez les options de l'instance Spot dans le paramètre `--instance-market-options`.

```
aws ec2 run-instances \  
  --image-id ami-0abcdef1234567890 \  
  --instance-market-options
```

```
--instance-type t2.micro \  
--count 5 \  
--subnet-id subnet-08fc749671b2d077c \  
--key-name MyKeyPair \  
--security-group-ids sg-0b0384b66d7d692f9 \  
--instance-market-options file://spot-options.json
```

Voici la structure de données à spécifier dans le fichier JSON pour `--instance-market-options`. Vous pouvez également spécifier `ValidUntil` et `InstanceInterruptionBehavior`. Si vous ne spécifiez pas de champ dans la structure de données, la valeur par défaut est utilisée.

L'exemple suivant crée une demande persistente.

```
{  
  "MarketType": "spot",  
  "SpotOptions": {  
    "SpotInstanceType": "persistent"  
  }  
}
```

Pour créer une demande d'instance Spot à l'aide de [request-spot-instances](#)

Note

Nous déconseillons fortement l'utilisation de la commande [request-spot-instances](#) pour demander une instance Spot, car il s'agit d'une API héritée qui ne fait l'objet d'aucun investissement prévu. Pour plus d'informations, consultez [Quelle est la meilleure méthode de demande Spot à utiliser ?](#)

Utilisez la commande [request-Spot-instances](#) pour créer une demande unique.

```
aws ec2 request-spot-instances \  
  --instance-count 5 \  
  --type "one-time" \  
  --launch-specification file://specification.json
```

Utilisez la commande [request-Spot-instances](#) pour créer une demande persistante.

```
aws ec2 request-spot-instances \  
  --instance-count 5 \  
  --type "persistent" \  
  --launch-specification file://specification.json
```

Pour accéder à des exemples de fichiers de spécification à utiliser avec ces commandes, consultez [Exemple de spécifications de lancement d'une demande d'instance Spot](#). Si vous téléchargez un fichier de spécification de lancement à partir de la console Spot Requests, vous devez utiliser la commande [request-spot-fleet](#) à la place (la console Spot Requests spécifie une demande d'instance Spot en utilisant un parc d'instances Spot).

Trouvez vos instances Spot

Amazon EC2 lance une instance Spot lorsque la capacité est disponible. Une instance Spot s'exécute jusqu'à ce qu'elle soit interrompue ou que vous la résilieez.

Une instance Spot apparaît sur la page Instances de la console, avec les instances à la demande. Utilisez la procédure suivante pour trouver vos instances Spot.

Console

Pour trouver vos instances Spot à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Pour trouver toutes les instances Spot, dans le volet de recherche, choisissez Instance lifecycle=spot.
4. Pour vérifier qu'une instance est une instance ponctuelle, sélectionnez l'instance, cliquez sur l'onglet Détails et vérifiez la valeur de Lifecycle. La valeur d'une instance ponctuelle est spot et la valeur d'une instance à la demande est normal.

AWS CLI

Pour trouver vos instances Spot à l'aide du AWS CLI

Utilisez la commande [describe-instances](#) avec l'option `--filters`.

```
aws ec2 describe-instances \  
  --filters
```

```
--filters "Name=instance-lifecycle,Values=spot"
```

Pour déterminer si une instance est une instance ponctuelle

Utilisez la commande [describe-instances](#), en utilisant l'option `--query` permettant de vérifier la valeur du cycle de vie.

```
aws ec2 describe-instances \  
  --instance-ids i-0123a456700123456 \  
  --query "Reservations[*].Instances[*].InstanceLifecycle" \  
  --output text
```

Si le résultat est `spot`, l'instance est une instance Spot. S'il n'y a aucune sortie, l'instance est une instance à la demande.

Utilisez la procédure suivante pour rechercher les instances Spot lancées à partir d'une demande d'instance Spot ou de flotte Spot spécifique.

Console

Pour trouver les instances Spot pour une demande à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot. La liste contient à la fois les demandes d'instance Spot et les demandes de parc Spot.
3. Si une demande d'instance Spot est satisfaite, Capacity est l'ID de l'instance Spot. Pour un parc d'instances Spot, le champ Capacité indique la part de la capacité demandée qui a été satisfaite. Pour afficher les ID des instances d'un parc d'instances Spot, choisissez la flèche de développement, ou sélectionnez le parc et choisissez Instances.
4. Pour une flotte ponctuelle, la capacité indique la quantité de capacité demandée qui est atteinte. Pour afficher les identifiants des instances d'un parc Spot, choisissez l'ID du parc pour ouvrir sa page de détails et localiser le volet Instances.

AWS CLI

Pour trouver les instances ponctuelles pour une demande à l'aide du AWS CLI

Utilisez la commande [describe-spot-instance-requests](#) avec l'option `--query`

```
aws ec2 describe-spot-instance-requests \  
  --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

Voici un exemple de sortie :

```
[  
  {  
    "ID": "i-1234567890abcdef0"  
  },  
  {  
    "ID": "i-0598c7d356eba48d7"  
  }  
]
```

Marquer les demandes d'instance Spot

Pour vous aider à classer et à gérer vos demandes d'instance Spot, vous pouvez les marquer avec des métadonnées personnalisées. Vous pouvez affecter une balise à une demande d'instance Spot lorsque vous la créez, ou après. Vous pouvez attribuer des balises à l'aide de la console Amazon EC2 ou d'un outil de ligne de commande.

Lorsque vous balisez une demande d'instance Spot, les instances et les volumes lancés par la demande d'instance Spot ne sont pas automatiquement balisés. Vous devez baliser explicitement les instances et les volumes lancés par la demande d'instance Spot. Vous pouvez affecter une balise à une instance Spot et à des volumes pendant le lancement, ou après.

Pour plus d'informations sur le fonctionnement des balises, consultez [Baliser vos ressources Amazon EC2](#).

Table des matières

- [Prérequis](#)
- [Baliser une nouvelle demande d'instance Spot](#)
- [Baliser une demande d'instance Spot existante](#)
- [Afficher les balises de demande d'instance Spot](#)

Prérequis

Octroyez à l'utilisateur l'autorisation de baliser les ressources. Pour plus d'informations sur les stratégies IAM et les exemples de stratégies, consultez [Exemple : Baliser des ressources](#).

La politique IAM que vous créez est déterminée par la méthode que vous utilisez pour créer une demande d'instance Spot.

- Si vous utilisez l'assistant de lancement d'instance ou `run-instances` pour demander Instances Spot, consultez [To grant a user the permission to tag resources when using the launch instance wizard or run-instances](#).
- Si vous utilisez la commande `request-spot-instances` pour demander des instances Spot, consultez [To grant a user the permission to tag resources when using request-spot-instances](#).

Pour accorder à un utilisateur l'autorisation de baliser des ressources lors de l'utilisation de l'assistant de lancement d'instance ou de `run-instances`

Créez une politique IAM qui inclut les éléments suivants :

- L'action `ec2:RunInstances`. Cela accorde à l'utilisateur l'autorisation de lancer une instance.
- Pour `Resource`, spécifiez `spot-instances-request`. Cela permet aux utilisateurs de créer des demandes d'instance Spot, qui demandent des instances Spot.
- L'action `ec2:CreateTags`. Celle-ci accorde à l'utilisateur l'autorisation de créer des balises.
- Pour `Resource`, spécifiez `*`. Cela permet aux utilisateurs de baliser toutes les ressources créées lors du lancement de l'instance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLaunchInstances",
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1::image/*",
        "arn:aws:ec2:us-east-1:*:subnet/*",

```

```

        "arn:aws:ec2:us-east-1:*:network-interface/*",
        "arn:aws:ec2:us-east-1:*:security-group/*",
        "arn:aws:ec2:us-east-1:*:key-pair/*",
        "arn:aws:ec2:us-east-1:*:volume/*",
        "arn:aws:ec2:us-east-1:*:instance/*",
        "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
    ]
},
{
    "Sid": "TagSpotInstanceRequests",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "*"
}
]
}

```

Lorsque vous utilisez cette RunInstances action pour créer des demandes d'instance ponctuelle et que vous balisez les demandes d'instance ponctuelle lors de leur création, vous devez savoir comment Amazon EC2 évalue la `spot-instances-request` ressource dans la RunInstances déclaration selon laquelle elle est évaluée dans la politique IAM comme suit :

- Si vous ne balisez pas une demande d'instance Spot lors de la création, Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la RunInstances déclaration.
- Si vous balisez une demande d'instance Spot lors de la création, Amazon EC2 évalue la `spot-instances-request` ressource dans le relevé. RunInstances

Par conséquent, pour la ressource `spot-instances-request`, les règles suivantes s'appliquent à la stratégie IAM :

- Si vous avez l' RunInstances habitude de créer une demande d'instance ponctuelle et que vous n'avez pas l'intention de baliser la demande d'instance ponctuelle lors de la création, vous n'avez pas besoin d'autoriser explicitement la `spot-instances-request` ressource ; l'appel aboutira.
- Si vous avez l' RunInstances habitude de créer une demande d'instance Spot et que vous avez l'intention de baliser la demande d'instance Spot lors de sa création, vous devez inclure la `spot-instances-request` ressource RunInstances dans l'instruction d'autorisation, sinon l'appel échouera.
- Si vous avez l' RunInstances habitude de créer une demande d'instance Spot et que vous avez l'intention de baliser la demande d'instance Spot lors de sa création, vous devez spécifier la

spot-instances-request ressource ou inclure un * caractère générique dans CreateTags l'instruction d'autorisation, sinon l'appel échouera.

Par exemple, pour les politiques IAM, y compris les politiques qui ne sont pas prises en charge pour les demandes d'instance Spot, consultez [Utiliser instances Spot](#).

Pour accorder à un utilisateur l'autorisation de baliser des ressources lors de l'utilisation d'instances request-spot-instances

Créez une politique IAM qui inclut les éléments suivants :

- L'action ec2:RequestSpotInstances. Cela accorde à l'utilisateur l'autorisation de créer une demande d'instance Spot.
- L'action ec2:CreateTags. Celle-ci accorde à l'utilisateur l'autorisation de créer des balises.
- Pour Resource, spécifiez spot-instances-request. Cela permet aux utilisateurs de baliser uniquement la demande d'instance Spot.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "TagSpotInstanceRequest",
      "Effect": "Allow",
      "Action": [
        "ec2:RequestSpotInstances",
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-request/*"
    }
  ]
}
```

Baliser une nouvelle demande d'instance Spot

Console

Pour baliser une nouvelle demande d'instance Spot à l'aide de la console

1. Suivez la procédure [Créer une demande d'instance Spot](#).

2. Pour ajouter une balise, sur la page Ajouter des balises , choisissez Ajouter une balise, puis entrez la clé et la valeur de la balise. Choisissez Ajouter une autre balise pour chaque balise supplémentaire.

Pour chaque balise, vous pouvez baliser la demande d'instance Spot, les instances Spot et les volumes avec la même balise. Pour baliser les trois, assurez-vous que instances, Volumes, et Demandes d'instance Spot sont sélectionnés. Pour n'en baliser qu'une ou deux, assurez-vous que les ressources que vous souhaitez baliser sont sélectionnées et que les autres ressources sont effacées.

3. Remplissez les champs obligatoires pour créer une demande d'instance Spot, puis choisissez Lancer. Pour plus d'informations, consultez [Créer une demande d'instance Spot](#).

AWS CLI

Pour étiqueter une nouvelle demande d'instance Spot à l'aide du AWS CLI

Pour étiqueter une demande d'instance Spot lors de sa création, configurez la demande d'instance Spot comme suit :

- Spécifiez les balises de la demande d'instance Spot à l'aide du paramètre `--tag-specification`.
- Pour `ResourceType`, spécifiez `spot-instances-request`. Si vous indiquez une autre valeur, la demande d'instance Spot échouera.
- Pour `Tags`, spécifiez la paire clé-valeur. Vous pouvez définir plus d'une paire clé-valeur.

Dans l'exemple suivant, la demande d'instance Spot est marquée par deux balises : `Key=Environment` et `Value=Production`, ainsi que `Key=Cost-Center` et `Value=123`.

```
aws ec2 request-spot-instances \  
  --instance-count 5 \  
  --type "one-time" \  
  --launch-specification file://specification.json \  
  --tag-specification 'ResourceType=spot-instances-  
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

Baliser une demande d'instance Spot existante

Console

Pour baliser une demande d'instance Spot existante à l'aide de la console

Après avoir créé une demande d'instance Spot, vous pouvez ajouter des balises à la demande d'instance Spot à l'aide de la console.

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande d'instance Spot.
4. Choisissez l'onglet Tags (Balises), puis Create Tag (Créer une balise).

Pour baliser une instance Spot existante à l'aide de la console

Une fois que votre demande d'instance Spot a lancé votre instance Spot, vous pouvez ajouter des balises à l'instance à l'aide de la console. Pour plus d'informations, consultez [Ajouter et supprimer des balises pour une ressource individuelle](#).

AWS CLI

Pour baliser une demande d'instance Spot ou une instance Spot existante à l'aide du AWS CLI

Utilisez la commande [create-tags](#) pour baliser les ressources existantes. Dans l'exemple suivant, la demande d'instance Spot existante et l'instance Spot sont balisées avec Key=purpose et Value=test.

```
aws ec2 create-tags \  
  --resources sir-08b93456 i-1234567890abcdef0 \  
  --tags Key=purpose,Value=test
```

Afficher les balises de demande d'instance Spot

Console

Pour afficher les balises d'une demande d'instance Spot à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.

3. Sélectionnez votre demande d'instance Spot et choisissez l'onglet Balises.

AWS CLI

Pour décrire les balises de demande d'instance Spot

Vous pouvez consulter les balises d'une demande d'instance Spot en décrivant la demande d'instance Spot. Utilisez la commande [describe-spot-instance-requests](#) pour afficher la configuration de la demande d'instance Spot spécifiée, qui inclut toutes les balises définies pour la demande.

```
aws ec2 describe-spot-instance-requests \  
  --spot-instance-request-ids sir-EXAMPLE1 \  
  --query "SpotInstanceRequests[*].Tags"
```

Voici un exemple de sortie.

```
[  
  [  
    {  
      "Key": "Environment",  
      "Value": "Production"  
    },  
    {  
      "Key": "Department",  
      "Value": "101"  
    }  
  ]  
]
```

Annuler une demande d'instance Spot

Si vous n'avez plus besoin de votre demande d'instance Spot, vous pouvez l'annuler. Vous pouvez annuler que les demandes d'instances Spot qui sont open, active, ou disabled.

- Votre demande d'instance Spot est open lorsqu'elle n'a pas encore été exécutée et si aucune instance n'a été lancée.
- Votre demande d'instance Spot est active lorsqu'elle a été satisfaite et que les instances Spot ont été lancées en conséquence.

- Votre demande d'instance Spot est `disabled` lorsque vous arrêtez votre instance Spot.

Si votre demande d'instance Spot est active et qu'elle est associée à une instance Spot en cours d'exécution, l'annulation de la demande ne résilie pas l'instance. Pour plus d'informations sur la résiliation d'une instance Spot, consultez [Résilier une instance Spot](#).

Console

Pour annuler une demande d'instance Spot à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez la demande d'instance Spot.
4. Choisissez Actions, Annuler la demande.
5. (Facultatif) Si vous n'avez plus besoin d'utiliser les instances Spot associées, vous pouvez les résilier. Dans la boîte de dialogue Annuler la demande Spot sélectionnez Terminer les instances, puis choisissez Confirmer.

AWS CLI

Pour annuler une demande d'instance Spot à l'aide du AWS CLI

Utilisez la commande [cancel-spot-instance-requests](#) pour annuler la demande d'instance Spot spécifiée.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Arrêt d'une instance Spot

Si vous n'avez pas besoin de vos instances Spot actuellement, mais que vous souhaitez les redémarrer plus tard sans perdre les données persistantes du volume Amazon EBS, vous pouvez les arrêter. Les étapes d'arrêt d'une instance Spot sont similaires à celles de l'arrêt d'une instance à la demande.

Note

Pendant qu'une instance Spot est arrêtée, vous pouvez modifier certains de ses attributs, mais pas le type d'instance.

Nous ne vous facturons pas l'utilisation d'une instance Spot arrêtée, ni les frais de transfert de données, mais nous facturons le stockage des volumes Amazon EBS.

Limites

- Vous ne pouvez arrêter une instance Spot que si elle a été lancée à partir d'une demande d'instance Spot persistant.
- Vous ne pouvez pas arrêter une instance Spot si la demande d'instance Spot associée est annulée. Lorsque la demande d'instance Spot est annulée, vous ne pouvez que résilier l'instance Spot.
- Vous ne pouvez pas arrêter une instance Spot si elle fait partie d'une flotte, d'un groupe de lancement ou d'un groupe de zone de disponibilité.

Console

Pour arrêter une instance Spot à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance Spot. Si vous n'avez pas enregistré l'ID d'instance de l'instance Spot, consultez [the section called “Trouvez vos instances Spot”](#).
4. Choisissez État de l'instance, Arrêter l'instance.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter.

AWS CLI

Pour arrêter une instance Spot à l'aide du AWS CLI

Utilisez la commande [stop-instances](#) pour arrêter manuellement vos instances Spot.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

Démarrer une instance Spot

Vous pouvez démarrer une instance Spot que vous avez précédemment arrêtée.

Prérequis

Vous pouvez démarrer une instance Spot uniquement si :

- Vous avez manuellement arrêté l'instance Spot.
- L'instance Spot est une instance basée sur EBS.
- La capacité d'instance Spot est disponible.
- Le prix Spot est inférieur à votre prix maximum.

Limites

- Vous ne pouvez pas démarrer une instance Spot qui fait partie d'une flotte, d'un groupe de lancement ou d'un groupe de zone de disponibilité.

Les étapes du démarrage d'une instance Spot sont similaires à celles du démarrage d'une instance à la demande.

Console

Pour démarrer une instance Spot à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance Spot. Si vous n'avez pas enregistré l'ID d'instance de l'instance Spot, consultez [the section called "Trouvez vos instances Spot"](#).
4. Choisissez État de l'instance, Démarrer l'instance.

AWS CLI

Pour démarrer une instance Spot, AWS CLI

Utilisez la commande [start-instances](#) pour démarrer manuellement vos instances Spot.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

Résilier une instance Spot

Si vous résiliez une instance Spot en cours d'exécution ou arrêtée qui a été lancée par une demande d'instance Spot persistante, la demande d'instance Spot passe à l'état open pour qu'une nouvelle instance Spot puisse être lancée. Pour vous assurer qu'aucune nouvelle instance Spot ne soit lancée, vous devez d'abord annuler la demande d'instance Spot.

Si vous annulez une demande d'instance Spot active qui comporte une instance Spot en cours d'exécution, celle-ci n'est pas résiliée automatiquement. Vous devez la résilier manuellement.

Si vous annulez une demande d'instance Spot disabled qui a une instance Spot arrêtée, le service Spot Amazon EC2 résilie celle-ci automatiquement. Il peut y avoir un bref décalage entre le moment où vous annulez la demande d'instance Spot et celui où le service Spot résilie l'instance Spot.

Pour plus d'informations, consultez [Annuler une demande d'instance Spot](#).

Console

Pour résilier manuellement une instance Spot à l'aide de la console

1. Avant de résilier une instance, vérifiez que vous ne perdrez aucune donnée en vous assurant que vos volumes Amazon EBS ne seront pas supprimés lors de la résiliation et que vous avez copié les données dont vous avez besoin des volumes du stockage d'instances vers un stockage persistant, par exemple Amazon EBS ou Amazon S3.
2. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
3. Dans le panneau de navigation, sélectionnez Instances.
4. Sélectionnez l'instance Spot. Si vous n'avez pas enregistré l'ID d'instance de l'instance Spot, consultez [the section called "Trouvez vos instances Spot"](#).
5. Choisissez État de l'instance, Résilier l'instance.
6. Choisissez Résilier lorsque vous êtes invité à confirmer.

AWS CLI

Pour mettre fin manuellement à une instance Spot à l'aide du AWS CLI

Utilisez la commande [terminate-instances](#) pour mettre fin manuellement à vos instances Spot.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

Exemple de spécifications de lancement d'une demande d'instance Spot

Les exemples suivants montrent les configurations de lancement que vous pouvez utiliser avec la commande [request-spot-instances](#) afin de créer une demande d'instance Spot. Pour plus d'informations, consultez [Créer une demande d'instance Spot](#).

Important

Nous déconseillons fortement l'utilisation de la commande [request-spot-instances](#) pour demander une instance Spot, car il s'agit d'une API héritée qui ne fait l'objet d'aucun investissement prévu. Pour plus d'informations, voir [Quelle est la meilleure méthode de demande Spot à utiliser ?](#)

Exemples

- [Exemple 1 : Lancement d'instances Spot](#)
- [Exemple 2 : Lancement d'instances Spot dans la zone de disponibilité spécifiée](#)
- [Exemple 3 : Lancement d'instances Spot dans le sous-réseau spécifié](#)
- [Exemple 4 : Lancement d'une instance Spot dédiée](#)

Exemple 1 : Lancement d'instances Spot

L'exemple suivant n'inclut aucune zone de disponibilité ou sous-réseau. Amazon EC2 sélectionne une zone de disponibilité pour vous. Amazon EC2 lance les instances sur le sous-réseau par défaut de la zone de disponibilité sélectionnée.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "IamInstanceProfile": {
    "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Exemple 2 : Lancement d'instances Spot dans la zone de disponibilité spécifiée

L'exemple suivant inclut une zone de disponibilité. Amazon EC2 lance les instances dans le sous-réseau par défaut de la zone de disponibilité spécifiée.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
    "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Exemple 3 : Lancement d'instances Spot dans le sous-réseau spécifié

L'exemple suivant inclut un sous-réseau. Amazon EC2 lance les instances dans le sous-réseau spécifié. S'il s'agit d'un VPC personnalisé, l'instance ne reçoit pas d'adresse IPv4 publique par défaut.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
    "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Pour attribuer une adresse IPv4 publique à une instance sur un VPC personnalisé, spécifiez le champ `AssociatePublicIpAddress` tel qu'illustré à l'exemple suivant. Lorsque vous spécifiez une interface réseau, vous devez inclure l'ID du sous-réseau et l'ID du groupe de sécurité à l'aide de l'interface réseau au lieu d'utiliser les champs `SubnetId` et `SecurityGroupIds` illustrés dans le bloc de code précédent.

```
{
```

```
"ImageId": "ami-0abcdef1234567890",
"KeyName": "my-key-pair",
"InstanceType": "m5.medium",
"NetworkInterfaces": [
  {
    "DeviceIndex": 0,
    "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
    "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
    "AssociatePublicIpAddress": true
  }
],
"IamInstanceProfile": {
  "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
}
}
```

Exemple 4 : Lancement d'une instance Spot dédiée

L'exemple suivant demande une instance Spot avec une location de `dedicated`. Une instance Spot dédiée doit être lancée sur un VPC.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Statut des demandes Spot

Pour vous aider à assurer le suivi de vos demandes d'instance Spot et à planifier votre utilisation d'instances Spot, utilisez l'état de demande fourni par Amazon EC2. Par exemple, le statut de la demande peut indiquer pourquoi votre demande d'instance Spot n'a pas encore été satisfaite, ou répertorier les contraintes qui empêchent l'exécution de votre demande d'instance Spot.

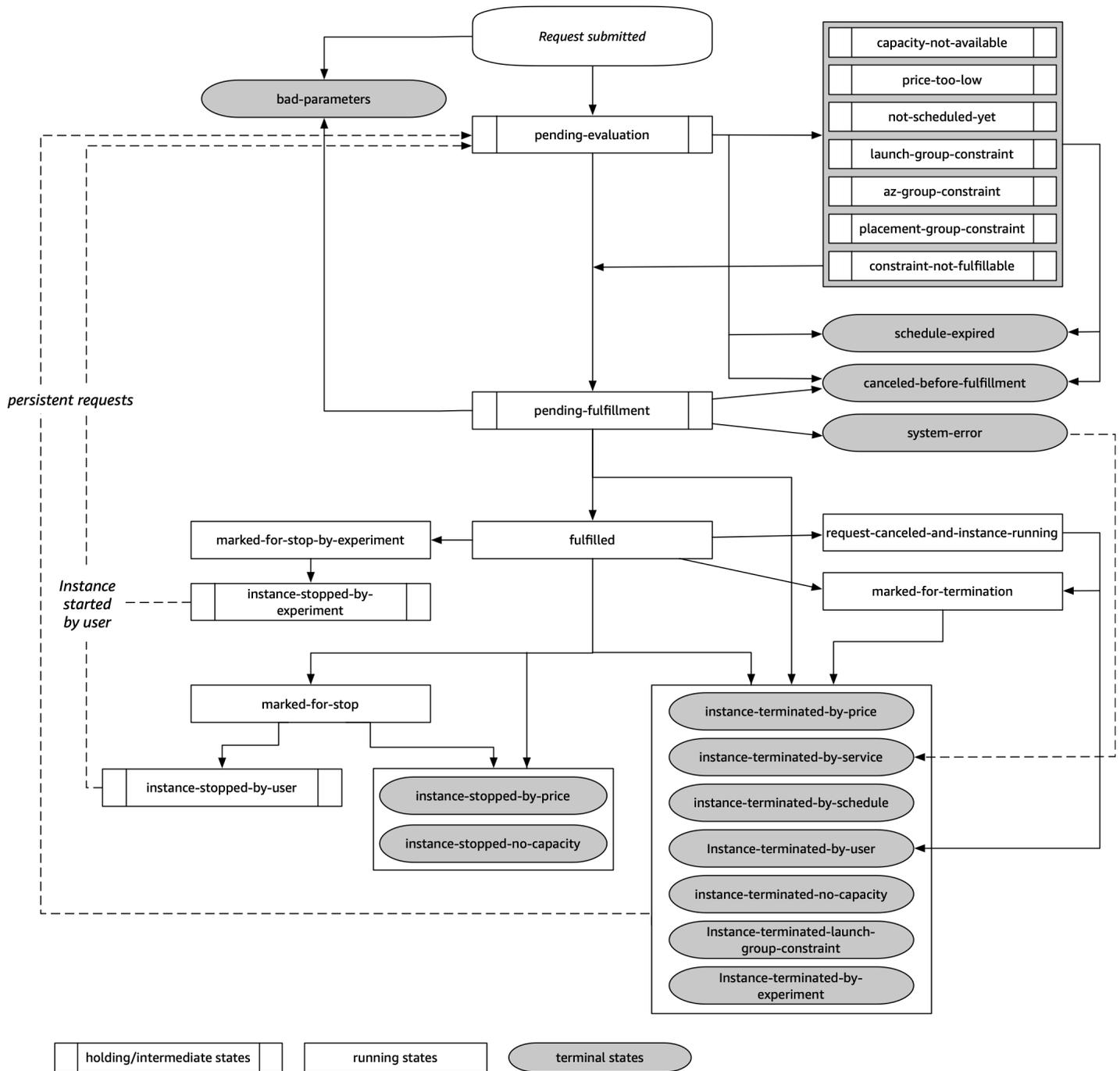
À chaque étape du processus, c'est-à-dire au cours du cycle de vie d'une demande Spot, des événements spécifiques déterminent les états successifs de la demande.

Sommaire

- [Cycle de vie d'une demande Spot](#)
- [Obtenir des informations sur le statut d'une demande](#)
- [Codes de statut des demandes Spot](#)
- [Événement d'exécution de demande d'instance Spot EC2](#)

Cycle de vie d'une demande Spot

Le diagramme suivant illustre les étapes suivies par votre demande d'instance Spot au cours de son cycle de vie, de la soumission à la mise hors service. Chaque étape est représentée sous forme d'un nœud et le code de statut de chaque nœud décrit le statut de la demande d'instance Spot et de l'instance Spot.



Évaluation en attente

Dès que vous créez une demande d'instance Spot, celle-ci passe à l'état pending-evaluation à moins qu'un ou plusieurs paramètres de demande ne soient pas valides (bad-parameters).

Code d'état	État de la demande	État de l'instance
pending-evaluation	open	Ne s'applique pas
bad-parameters	closed	Ne s'applique pas

En attente

Si une ou plusieurs contraintes de demande sont valides mais ne peuvent pas encore être respectées ou s'il n'y a pas suffisamment de capacité, la demande se voit attribuer l'état En attente jusqu'à ce que les contraintes soient respectées. Les options de la demande ont un impact sur les possibilités d'exécution de la demande. Par exemple, si la capacité n'est pas disponible, votre demande reste à l'état en attente jusqu'à ce que la capacité devienne disponible. Si vous spécifiez un groupe de zone de disponibilité, la demande conserve l'état En attente jusqu'à ce que la contrainte de zone de disponibilité soit respectée.

En cas de panne de l'une des zones de disponibilité, il est possible que la capacité EC2 disponible pour les demandes d'instance Spot dans d'autres zones de disponibilité puisse être affectée.

Code d'état	État de la demande	État de l'instance
capacity-not-available	open	Ne s'applique pas
price-too-low	open	Ne s'applique pas
not-scheduled-yet	open	Ne s'applique pas
launch-group-constraint	open	Ne s'applique pas
az-group-constraint	open	Ne s'applique pas
placement-group-constraint	open	Ne s'applique pas

Code d'état	État de la demande	État de l'instance
<code>constraint-not-fulfillable</code>	<code>open</code>	Ne s'applique pas

Fin de l'évaluation/exécution-terminal

Votre demande d'instance Spot peut passer à l'état `terminal` si vous créez une demande valide uniquement pendant une durée spécifique et que cette durée arrive à expiration avant que votre demande atteigne la phase d'exécution en attente. Cela peut également se produire si vous annulez la demande ou si une erreur système se produit.

Code d'état	État de la demande	État de l'instance
<code>schedule-expired</code>	<code>cancelled</code>	Ne s'applique pas
<code>cancel-before-fulfillment</code> ¹	<code>cancelled</code>	Ne s'applique pas
<code>bad-parameters</code>	<code>failed</code>	Ne s'applique pas
<code>system-error</code>	<code>closed</code>	Ne s'applique pas

¹ Si vous annulez la demande.

Exécution en attente

Lorsque les contraintes que vous avez spécifiées (le cas échéant) sont respectées, votre demande Spot passe à l'état `pending-fulfillment`.

A ce stade, Amazon EC2 est prêt à mettre en service les instances que vous avez demandées. Si le processus s'arrête à ce stade, il a probablement été annulé par l'utilisateur avant le lancement d'une instance Spot. Cela peut aussi être dû à une erreur système inattendue.

Code d'état	État de la demande	État de l'instance
pending-fulfillment	open	Ne s'applique pas

Exécutée

Lorsque toutes les caractéristiques de vos instances Spot sont respectées, votre demande d'instance Spot est satisfaite. Amazon EC2 lance les instances Spot, ce qui peut prendre quelques minutes. Si une instance Spot est mise en veille prolongée ou arrêtée lorsqu'elle est interrompue, elle reste dans cet état jusqu'à ce que la demande puisse être de nouveau satisfaite ou qu'elle soit annulée.

Code d'état	État de la demande	État de l'instance
fulfilled	active	pending → running
fulfilled	active	stopped → running

Si vous arrêtez une instance Spot, votre demande Spot passe à l'état `marked-for-stop` ou `instance-stopped-by-user` jusqu'à ce que l'instance Spot puisse être redémarrée ou que la demande soit annulée.

Code d'état	État de la demande	État de l'instance
marked-for-stop	active	stopping
instance-stopped-by-user ¹	disabled ou cancelled ²	stopped

¹ Une instance Spot passe à l'état `instance-stopped-by-user` si vous arrêtez l'instance ou si vous exécutez la commande `shutdown` à partir de l'instance. Une fois l'instance arrêtée, vous pouvez la redémarrer. Au redémarrage, la demande d'instance Spot revient à l'état `pending-evaluation`, puis Amazon EC2 lance une nouvelle instance Spot lorsque les exigences sont respectées.

² L'état de la demande Spot est `disabled` si vous arrêtez l'instance Spot sans annuler la demande. L'état de la demande est `cancelled` si votre instance Sport est arrêtée et que la demande expire.

Exécuté-terminal

Vos instances Spot continuent de s'exécuter tant qu'il existe de la capacité pour votre type d'instance et que vous ne résiliez pas l'instance. Si Amazon EC2 doit résilier vos instances Spot, la demande Spot passe à l'état terminal. Une demande se voit attribuer l'état terminal si vous annulez la demande Spot ou si vous résiliez les instances Spot.

Code d'état	État de la demande	État de l'instance
request-canceled-and-instance-running	cancelled	running
marked-for-stop	active	running
marked-for-termination	active	running
instance-stopped-by-price	disabled	stopped
instance-stopped-by-user	disabled	stopped
instance-stopped-no-capacity	disabled	stopped
instance-terminated-by-price	closed (exceptionnelle), open (persistante)	terminated
instance-terminated-by-schedule	closed	terminated
instance-terminated-by-service	cancelled	terminated
instance-terminated-by-user	closed ou cancelled ¹	terminated
instance-terminated-no-capacity	closed (exceptionnelle), open (persistante)	running †

Code d'état	État de la demande	État de l'instance
<code>instance-terminated-no-capacity</code>	<code>closed</code> (exceptionnelle), <code>open</code> (persistante)	<code>terminated</code>
<code>instance-terminate-d-launch-group-constraint</code>	<code>closed</code> (exceptionnelle), <code>open</code> (persistante)	<code>terminated</code>

¹ L'état de la demande est `closed` si vous résiliez l'instance, mais que vous n'annulez pas la demande. L'état de la demande est `cancelled` si vous mettez l'instance hors service et que vous annulez la demande. Même si vous résiliez une instance Spot avant d'annuler sa demande, un certain laps de temps peut s'écouler avant qu'Amazon EC2 ne détecte la résiliation de votre instance Spot. Le cas échéant, l'état `closed` ou `cancelled` est attribué à la demande.

† Quand Amazon EC2 interrompt une instance Spot si elle a besoin de récupérer la capacité et que l'instance est configurée pour être résiliée en cas d'interruption, le statut est immédiatement défini sur `instance-terminated-no-capacity` (il n'est pas défini sur `marked-for-termination`). Toutefois, l'instance reste dans à l'état `running` pendant 2 minutes pour refléter la période de 2 minutes pendant laquelle elle reçoit l'avis d'interruption de l'instance Spot. Au bout de 2 minutes, l'état de l'instance est défini sur `terminated`.

Expériences d'interruption

Vous pouvez l'utiliser AWS Fault Injection Service pour déclencher une interruption d'instance Spot afin de tester la façon dont les applications de vos instances Spot répondent. Si AWS FIS une instance Spot est arrêtée, votre demande Spot entre dans l'`marked-for-stop-by-experiment` état puis dans l'`instance-stopped-by-experiment` état. En cas de AWS FIS résiliation d'une instance Spot, votre demande Spot entre dans l'`instance-terminated-by-experiment` état. Pour plus d'informations, consultez [the section called "Initier une interruption"](#).

Code d'état	État de la demande	État de l'instance
<code>marked-for-stop-by-experiment</code>	<code>active</code>	<code>running</code>

Code d'état	État de la demande	État de l'instance
<code>instance-stopped-by-experiment</code>	<code>disabled</code>	<code>stopped</code>
<code>instance-terminated-by-experiment</code>	<code>closed</code>	<code>terminated</code>

Demandes persistantes

Lorsque vos instances Spot sont résiliées (soit par vous, soit par Amazon EC2), si la demande Spot est une demande persistante, elle retourne à l'état `pending-evaluation` et Amazon EC2 peut lancer une nouvelle instance Spot lorsque les exigences sont respectées.

Obtenir des informations sur le statut d'une demande

Vous pouvez obtenir des informations sur l'état de la demande à l'aide de l'outil AWS Management Console ou en ligne de commande.

Pour obtenir des informations sur le statut d'une demande à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Demandes Spot et sélectionnez la demande d'instance Spot.
3. Pour vérifier l'état, sous l'onglet Description, cochez le champ Statut.

Pour obtenir des informations sur le statut de la demande à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [describe-Spot-instance-requests](#) (AWS CLI)
- [Get-EC2SpotInstanceRequest](#) (AWS Tools for Windows PowerShell)

Codes de statut des demandes Spot

Les informations sur le statut des demandes Spot sont composées d'un code de statut, de l'heure de mise à jour et d'un message de statut. Toutes ces informations vous permettent de savoir où en est votre demande d'instance Spot.

Voici les codes de statut des demandes Spot :

az-group-constraint

Amazon EC2 ne peut pas lancer toutes les instances que vous avez demandées dans la même zone de disponibilité.

bad-parameters

Un ou plusieurs paramètres de votre demande d'instance Spot ne sont pas valides (par exemple, l'AMI que vous avez spécifiée n'existe pas). Le message de statut indique quel paramètre n'est pas valide.

anceled-before-fulfillment

L'utilisateur a annulé la demande d'instance Spot avant son exécution.

capacity-not-available

Il n'y a pas suffisamment de capacité disponible pour les instances que vous avez demandées.

constraint-not-fulfillable

La demande d'instance Spot ne peut pas être satisfaite dans la mesure où une ou plusieurs contraintes ne sont pas valides (par exemple, la zone de disponibilité n'existe pas). Le message de statut indique quelle contrainte n'est pas valide.

fulfilled

La demande Spot est active, et Amazon EC2 lance votre Instances Spot.

instance-stopped-by-price

Votre instance a été arrêtée car le prix Spot a dépassé votre prix maximum.

instance-stopped-by-user

Votre instance a été arrêtée car un utilisateur l'a arrêtée ou a exécuté la commande shutdown à partir de l'instance.

`instance-stopped-no-capacity`

Votre instance a été arrêtée en raison des besoins de gestion de la capacité EC2.

`instance-terminated-by-price`

Votre instance a été supprimée car le prix Spot a dépassé votre prix maximum. Si votre demande est une offre persistante, le processus redémarre et votre demande se retrouve en attente d'évaluation.

`instance-terminated-by-schedule`

Votre instance Spot a été résiliée à la fin de sa durée planifiée.

`instance-terminated-by-service`

Votre instance a été mise hors service à partir d'un état d'arrêt.

`instance-terminated-by-user` ou `spot-instance-terminated-by-user`

Étant donné que vous avez résilié une instance Spot qui a été exécutée, l'état de la demande est `closed` (sauf s'il s'agit d'une demande persistante) et l'état de l'instance est `terminated`.

`instance-terminated-launch-group-constraint`

Une ou plusieurs instances de votre groupe de lancement ont été mises hors service, c'est pourquoi la contrainte du groupe de lancement n'est plus respectée.

`instance-terminated-no-capacity`

Votre instance a été résiliée en raison de processus standard de gestion de la capacité.

`launch-group-constraint`

Amazon EC2 ne peut pas lancer toutes les instances que vous avez demandées en même temps. Toutes les instances d'un groupe de lancement sont démarrées et mises hors service ensemble.

`limit-exceeded`

La limite du nombre de volumes EBS ou du stockage de volume total a été dépassée. Pour plus d'informations sur ces limites et sur la manière de demander une augmentation, consultez [Limites d'Amazon EBS](#) (français non garanti) dans le Référence générale d'Amazon Web Services.

`marked-for-stop`

L'instance Spot est marquée pour être arrêtée.

`marked-for-termination`

L'instance Spot est marquée pour être résiliée.

not-scheduled-yet

La demande d'instance Spot n'est pas évaluée avant la date prévue.

pending-evaluation

Une fois que vous avez effectué une demande d'instance Spot, elle passe à l'état `pending-evaluation` le temps que le système évalue les paramètres de votre demande.

pending-fulfillment

Amazon EC2 tente d'allouer vos instances Spot.

placement-group-constraint

La demande Spot ne peut pas encore être satisfaite, car une instance Spot ne peut pas être ajoutée au groupe de placement à ce stade.

price-too-low

La demande ne peut pas encore être exécutée, car le prix maximum est inférieur au prix Spot. Dans le cas présent, aucune instance n'est lancée et votre demande reste à l'état `open`.

request-canceled-and-instance-running

Vous avez annulé la demande Spot alors que les instances Spot sont toujours en cours d'exécution. La demande est `cancelled`, tandis que les instances conservent l'état `running`.

schedule-expired

La demande d'instance Spot est arrivée à expiration car elle n'a pas été exécutée avant la date spécifiée.

system-error

Il y a eu une erreur système inattendue. S'il s'agit d'un problème récurrent, veuillez nous contacter AWS Support pour obtenir de l'aide.

Événement d'exécution de demande d'instance Spot EC2

Lorsqu'une demande d'instance Spot est traitée, Amazon EC2 envoie un événement de traitement de demande d'instance Spot EC2 à Amazon EventBridge. Vous pouvez créer une règle pour effectuer une action lorsque cet événement se produit, comme invoquer une fonction Lambda ou notifier une rubrique Amazon SNS.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "01234567-1234-0123-1234-012345678901",
  "detail-type": "EC2 Spot Instance Request Fulfillment",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-2",
  "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
  "detail": {
    "spot-instance-request-id": "sir-1a2b3c4d",
    "instance-id": "i-1234567890abcdef0"
  }
}
```

Pour plus d'informations, consultez le [guide de EventBridge l'utilisateur Amazon](#).

Recommandations de rééquilibrage des instances EC2

La recommandation de rééquilibrage d'instance EC2 vous permet d'être averti lorsqu'une instance Spot présente un risque élevé d'interruption. Le signal peut arriver plus tôt que l'[avis d'interruption d'instance Spot à deux minutes](#), ce qui vous donne la possibilité de gérer l'instance Spot de manière proactive. Vous pouvez décider de rééquilibrer votre charge de travail en une instances Spot nouvelle ou existante qui ne présente pas un risque élevé d'interruption.

Amazon EC2 n'est pas toujours capable d'envoyer le signal de recommandation de rééquilibrage avant l'avis d'interruption d'instance Spot de deux minutes. Par conséquent, le signal de recommandation de rééquilibrage peut arriver avec l'avis d'interruption de deux minutes.

Les recommandations de rééquilibrage sont mises à disposition sous forme d' EventBridge événement et d'élément dans les [métadonnées de l'instance](#) Spot. Les événements sont générés dans la mesure du possible.

Note

Les recommandations de rééquilibrage ne sont prises en charge que pour les instances Spot qui sont lancées après le 5 novembre 2020 00:00 UTC.

Rubriques

- [Actions de rééquilibrage que vous pouvez effectuer](#)
- [Surveiller les signaux de recommandation de rééquilibrage](#)
- [Services utilisant le signal de recommandation de rééquilibrage](#)

Actions de rééquilibrage que vous pouvez effectuer

Voici quelques-unes des actions de rééquilibrage possibles que vous pouvez effectuer :

Arrêt normal

Lorsque vous recevez le signal de recommandation de rééquilibrage pour une instance Spot, vous pouvez démarrer vos procédures d'arrêt d'instance, ce qui peut inclure la garantie que les processus sont terminés avant de les arrêter. Par exemple, vous pouvez charger des journaux système ou d'applications sur Amazon Simple Storage Service (Amazon S3), arrêter les travailleurs Amazon SQS ou terminer la désinscription du système de noms de domaine (DNS). Vous pouvez également enregistrer votre travail sur un stockage externe et le reprendre ultérieurement.

Empêcher la planification d'une nouvelle tâche

Lorsque vous recevez le signal de recommandation de rééquilibrage pour une instance Spot, vous pouvez empêcher la planification d'une nouvelle tâche sur l'instance, tout en continuant à utiliser l'instance jusqu'à ce que les tâches planifiées soient terminées.

Lancer de manière proactive de nouvelles instances de remplacement

Vous pouvez configurer des groupes Auto Scaling, une flotte EC2 ou un parc d'instances Spot pour lancer automatiquement des instances Spot de remplacement lorsqu'un signal de recommandation de rééquilibrage est émis. Pour plus d'informations, consultez [Utiliser le rééquilibrage de la capacité pour gérer les interruptions Spot Amazon EC2](#) (langue française non garantie) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling, ainsi que [Rééquilibrage de la capacité](#) pour le parc d'instances EC2 et [Rééquilibrage de la capacité](#) pour le parc d'instances Spot dans ce même guide de l'utilisateur.

Surveiller les signaux de recommandation de rééquilibrage

Vous pouvez surveiller le signal de recommandation de rééquilibrage afin que vous puissiez effectuer les actions spécifiées dans la section précédente lorsqu'il est émis. Le signal de recommandation de rééquilibrage est mis à disposition sous forme d'événement envoyé à Amazon EventBridge

(anciennement Amazon CloudWatch Events) et sous forme de métadonnées d'instance sur l'instance Spot.

Surveiller les signaux de recommandation de rééquilibrage :

- [Utilisez Amazon EventBridge](#)
- [Utiliser les métadonnées d'instance](#)

Utilisez Amazon EventBridge

Lorsque le signal de recommandation de rééquilibrage est émis pour une instance Spot, l'événement correspondant au signal est envoyé à Amazon EventBridge. S'il EventBridge détecte un modèle d'événement correspondant à un modèle défini dans une règle, EventBridge invoque une cible (ou des cibles) spécifiée dans la règle.

Voici un exemple d'événement pour le signal de recommandation de rééquilibrage.

```
{
  "version": "0",
  "id": "12345678-1234-1234-1234-123456789012",
  "detail-type": "EC2 Instance Rebalance Recommendation",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-2",
  "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
  "detail": {
    "instance-id": "i-1234567890abcdef0"
  }
}
```

Les champs suivants forment le modèle d'événement défini dans la règle :

"detail-type": "EC2 Instance Rebalance Recommendation"

Identifie que l'événement est un événement de recommandation de rééquilibrage

"source": "aws.ec2"

Identifie que l'événement provient de Amazon EC2

Création d'une EventBridge règle

Vous pouvez écrire une EventBridge règle et automatiser les actions à effectuer lorsque le modèle d'événement correspond à la règle.

L'exemple suivant crée une EventBridge règle pour envoyer un e-mail, un SMS ou une notification push mobile chaque fois qu'Amazon EC2 émet un signal de recommandation de rééquilibrage. Le signal est émis en tant qu'événement de EC2 Instance Rebalance Recommendation, ce qui déclenche l'action définie par la règle.

Avant de créer la EventBridge règle, vous devez créer la rubrique Amazon SNS pour l'e-mail, le message texte ou la notification push mobile.

Pour créer une EventBridge règle pour un événement de recommandation de rééquilibrage

1. Ouvrez la EventBridge console Amazon à l'[adresse https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Choisissez Créer une règle.
3. Pour Define rule detail (Définir les détails de la règle), procédez comme suit :

- a. Entrez un nom et éventuellement une description pour la règle.

Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

- b. Pour Event bus (Bus d'événement), choisissez default (défaut). Lorsqu'un service AWS de votre compte génère un événement, il accède toujours au bus d'événement par défaut de votre compte.
 - c. Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
 - d. Choisissez Suivant.
4. Pour Build event pattern (Créer un modèle d'événement), procédez comme suit :
 - a. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.
 - b. Pour le Event pattern (Modèle d'événement), dans cet exemple, spécifiez le modèle d'événement suivant pour correspondre à l'événement EC2 Instance Rebalance Recommendation, puis choisissez Save (Enregistrer).

```
{
```

```
"source": ["aws.ec2"],
"detail-type": ["EC2 Instance Rebalance Recommendation"]
}
```

Pour ajouter le modèle d'événement, vous pouvez utiliser un modèle en choisissant Event pattern form (Formulaire de modèle d'événement), ou spécifiez votre propre modèle en choisissant Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]), comme suit :

- i. Pour utiliser un modèle pour créer le modèle d'événement, procédez comme suit :
 - A. Sélectionnez Event pattern form (Formulaire de modèle d'événement).
 - B. Pour Event source (Origine de l'événement), choisissez AWS services (Services).
 - C. Pour Service AWS, choisissez Parc d'instances Spot EC2.
 - D. Pour Event type (Type d'événement), choisissez EC2 Instance Rebalance Recommendation (Recommandation de rééquilibrage des instances EC2).
 - E. Pour personnaliser le modèle, choisissez Edit pattern (Modifier le modèle) et apportez vos modifications pour correspondre à l'exemple de modèle d'événement.
 - ii. (Alternative) Pour spécifier un modèle d'événement personnalisé, procédez comme suit :
 - A. Choisissez Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]).
 - B. Dans la boîte de dialogue Event pattern (Modèle d'événement), ajoutez le modèle d'événement pour cet exemple.
- c. Choisissez Next (Suivant).
5. Pour Select target(s) (Sélectionner la ou les cibles), procédez comme suit :
- a. Pour Types de cibles, choisissez service AWS.
 - b. Pour Select a target (Sélectionner une cible), sélectionnez SNS topic (Rubrique SNS) pour envoyer un e-mail, un SMS ou une notification push mobile lorsque l'événement se produit.
 - c. Pour Topic (Rubrique), sélectionnez une rubrique existante. Vous devez d'abord créer une rubrique Amazon SNS à l'aide de la console Amazon SNS. Pour plus d'informations, consultez la section [Utilisation d'Amazon SNS pour la messagerie application-to-person \(A2P\) dans le manuel](#) du développeur Amazon Simple Notification Service.
 - d. (Facultatif) Sous Additional settings (Paramètres supplémentaires), vous pouvez configurer des paramètres supplémentaires. Pour plus d'informations, consultez la section [Création](#)

[de EventBridge règles Amazon réagissant aux événements](#) (étape 16) dans le guide de EventBridge l'utilisateur Amazon.

- e. Choisissez Suivant.
6. (Facultatif) Pour Tags (Identifications), vous pouvez également attribuer une ou plusieurs identifications à votre règle, puis choisir Next (Suivant).
7. Pour Review and create (Vérifier et créer), procédez comme suit :
 - a. Consultez les détails de la règle et modifiez-les si nécessaire.
 - b. Choisissez Créer une règle.

Pour plus d'informations, consultez les [EventBridge règles Amazon et les modèles d' EventBridge événements Amazon](#) dans le guide de EventBridge l'utilisateur Amazon

Utiliser les métadonnées d'instance

La catégorie de métadonnées d'instance `events/recommendations/rebalance` indique l'heure approximative, en UTC, à laquelle le signal de recommandation de rééquilibrage a été émis pour une instance Spot.

Nous vous recommandons de vérifier la présence de signaux de recommandation de rééquilibrage toutes les 5 secondes afin de ne pas manquer l'occasion de donner suite à la recommandation de rééquilibrage.

Si une instance Spot reçoit une recommandation de rééquilibrage, l'heure à laquelle le signal a été émis est présente dans les métadonnées de l'instance. Vous pouvez retrouver l'heure à laquelle le signal a été émis comme suit.

Utilisez la commande correspondant à votre système d'exploitation.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Voici un exemple de sortie, qui indique l'heure, en UTC, à laquelle le signal de recommandation de rééquilibrage a été émis pour l'instance Spot.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Si le signal n'a pas été émis pour l'instance, `events/recommendations/rebalance` n'est pas présent et vous recevez une erreur HTTP 404 lorsque vous essayez de le récupérer.

Services utilisant le signal de recommandation de rééquilibrage

Amazon EC2 Auto Scaling, la flotte EC2 et le parc d'instances Spot utilisent le signal de recommandation de rééquilibrage pour que vous puissiez facilement maintenir la disponibilité de la charge de travail en augmentant de manière proactive votre flotte avec une nouvelle instance Spot avant qu'une instance en cours ne reçoive l'avis d'interruption d'instance Spot à deux minutes. Vous pouvez demander à ces services de surveiller et de répondre de manière proactive aux changements affectant la disponibilité de votre instances Spot. Pour plus d'informations, consultez les ressources suivantes :

- [Utiliser le rééquilibrage de la capacité pour gérer les interruptions Spot Amazon EC2](#) (langue française non garantie) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling
- [Rééquilibrage de la capacité](#) dans la rubrique Flotte EC2 de ce guide de l'utilisateur
- [Rééquilibrage de la capacité](#) dans la rubrique Parc d'instances Spot de ce guide de l'utilisateur

Interruptions d'instance Spot

Vous pouvez lancer des instances Spot sur la capacité EC2 inutilisée et bénéficier de remises importantes si vous les renvoyez lorsque le service Amazon EC2 a à nouveau besoin de la capacité.

Lorsque Amazon EC2 réclame une instance Spot, nous appelons cet événement une interruption d'instance Spot.

Lorsqu'Amazon EC2 interrompt une instance Spot, il résilie, arrête ou met en veille prolongée l'instance, en fonction de ce que vous avez spécifié lors de la création de la demande Spot.

La demande d'instances Spot peut varier considérablement d'un instant à l'autre et la disponibilité des instances Spot peut également varier sensiblement selon le nombre d'instances EC2 disponibles qui ne sont pas utilisées. Il est toujours possible que votre instance Spot soit interrompue.

Une instance à la demande spécifiée dans une flotte EC2 ou un parc d'instances Spot ne peut pas être interrompue.

Table des matières

- [Raisons de l'interruption d'une instance Spot](#)
- [Comportement des interruptions des instances Spot](#)
- [Arrêter l'instances Spot interrompue](#)
- [Mettre les instances Spot interrompues en veille prolongée](#)
- [Résilier les instances Spot interrompues](#)
- [Préparez-vous aux interruptions des instances Spot](#)
- [Lancement d'une interruption d'instance Spot](#)
- [Avis d'interruption d'instance Spot.](#)
- [Identifier des instances Spot interrompues](#)
- [Déterminer si Amazon EC2 a résilié une instance Spot](#)
- [Facturation des instances Spot interrompues](#)

Raisons de l'interruption d'une instance Spot

Voici les raisons pour lesquelles Amazon EC2 est susceptible d'interrompre vos instances Spot :

Capacité

Amazon EC2 peut interrompre votre instance Spot lorsqu'il en a besoin. EC2 récupère votre instance la plupart du temps pour réaffecter la capacité, mais elle peut également la récupérer pour d'autres raisons telles que la maintenance de l'hôte ou la désaffectation du matériel.

Prix

Le prix Spot est supérieur à votre prix maximum.

Vous pouvez spécifier le prix maximum dans votre demande Spot. Cependant, si vous spécifiez un prix maximal, vos instances seront interrompues plus fréquemment que si vous ne le spécifiez pas.

Contraintes

Si votre demande comprend une exigence telle qu'un groupe de lancement ou un groupe de zone de disponibilité, les instances Spot sont résiliées en tant que groupe lorsque l'exigence n'est plus respectée.

Vous pouvez voir les taux d'interruption historiques de votre type d'instance dans la section [Conseiller d'instance Spot](#).

Comportement des interruptions des instances Spot

Vous pouvez spécifier qu'Amazon EC2 doit effectuer l'une des opérations suivantes lorsqu'il interrompt une instance Spot :

- [Arrêter l'instances Spot interrompue](#)
- [Mettre les instances Spot interrompues en veille prolongée](#)
- [Résilier les instances Spot interrompues](#) (il s'agit du comportement par défaut)

Spécifier le comportement d'interruption

Vous pouvez spécifier le comportement d'interruption lorsque vous créez une demande Spot. Si vous ne spécifiez pas de comportement d'interruption, par défaut, Amazon EC2 résilie les instances Spot lorsqu'elles sont interrompues.

La façon dont vous spécifiez le comportement d'interruption est différente selon la façon dont vous demandez instances Spot.

- Si vous effectuez une demande d'instances Spot à l'aide de [l'assistant de lancement d'instance](#), vous pouvez spécifier le comportement d'interruption comme suit : dans l'assistant de lancement d'instance, développez Détails avancés et cochez la case Demander des instances Spot. Choisissez Personnaliser. Dans Comportement d'interruption, choisissez un comportement

d'interruption. Si le comportement d'interruption est la mise en veille prolongée, vous pouvez également choisir Activer pour le champ Comportement d'arrêt - mise en veille prolongée.

- Si vous effectuez une demande d'instances Spot à l'aide de l'interface de ligne de commande [run-instances](#), vous pouvez spécifier le comportement d'interruption comme suit : dans la configuration de la demande, (`--instance-market-options`), pour `InstanceInterruptBehavior`, spécifiez un comportement d'interruption. Si le comportement d'interruption est la hibernation, vous pouvez également activer la mise en veille prolongée à l'aide du paramètre `--hibernation-options Configured=true`.
- Si vous configurez Instances Spot dans un [modèle de lancement](#), vous pouvez spécifier le comportement d'interruption comme suit : dans le modèle de lancement, développez Advanced details (Détails avancés) et cochez la case Request Instances Spot (Demande). Choisissez Personnaliser, puis, dans Comportement d'interruption, choisissez un comportement d'interruption.
- Si vous faites une demande Instances Spot à l'aide de la [console Spot](#), vous pouvez spécifier le comportement d'interruption comme suit : activez la case à cocher Maintenir la capacité cible puis, dans Comportement d'interruption, choisissez un comportement d'interruption.
- Si vous configurez des instances Spot dans la configuration de demande lors de l'utilisation de la CLI [create-fleet](#), vous pouvez spécifier le comportement d'interruption comme suit : pour `InstanceInterruptBehavior`, spécifiez un comportement d'interruption.
- Si vous configurez des instances Spot dans la configuration de demande lors de l'utilisation de la CLI [request-spot-fleet](#), vous pouvez spécifier le comportement d'interruption comme suit : pour `InstanceInterruptBehavior`, spécifiez un comportement d'interruption.
- Si vous configurez Instances Spot à l'aide de l'interface de ligne de commande [request-spot-instances](#) vous pouvez spécifier le comportement d'interruption comme suit : pour `--instance-interruption-behavior`, spécifiez un comportement d'interruption.

Note

Nous déconseillons fortement l'utilisation des commandes [request-spot-fleet](#) et [request-spot-instances](#) pour demander des instances Spot, car il s'agit d'API héritées qui ne font l'objet d'aucun investissement prévu. Pour plus d'informations, consultez [Quelle est la meilleure méthode de demande Spot à utiliser ?](#).

Arrêter l'instances Spot interrompue

Vous pouvez préciser qu'Amazon EC2 arrête vos instances Spot lorsqu'elles sont interrompues. Pour plus d'informations, consultez [Spécifier le comportement d'interruption](#).

Considérations

- Seul Amazon EC2 peut redémarrer une instance Spot arrêtée.
- Pour une instance Spot lancée par une demande d'instance Spot persistant : Amazon EC2 redémarre l'instance arrêtée quand la capacité est disponible dans la même zone de disponibilité et pour le même type d'instance que l'instance arrêtée (la même spécification de lancement doit être utilisée).
- Pour les instances Spot lancées par une flotte EC2 ou un parc d'instances Spot de type `maintain` : une fois qu'une instance Spot est interrompue, Amazon EC2 lance une instance de remplacement pour maintenir la capacité cible. Amazon EC2 trouve le ou les meilleurs groupe(s) de capacités Spot en fonction de la stratégie d'allocation spécifiée (`lowestPrice`, `diversified` ou `InstancePoolsToUseCount`). Il ne donne pas la priorité au groupe contenant l'instance résiliée le plus tôt. Ultérieurement, si la stratégie d'allocation conduit à un groupe contenant l'instances arrêtée le plus tôt, Amazon EC2 redémarre l'instance arrêtée pour assurer la capacité cible.

Par exemple, considérons un parc d'instances Spot avec la stratégie d'allocation `lowestPrice`. Lors du lancement initial, un pool `c3.large` répond aux critères `lowestPrice` pour la spécification de lancement. Ultérieurement, quand les instances `c3.large` sont interrompues, Amazon EC2 arrête les instances et réapprovisionne la capacité à partir d'un autre groupe adapté à la stratégie `lowestPrice`. Cette fois, le groupe est un groupe `c4.large` et Amazon EC2 lance des instances `c4.large` pour assurer la capacité cible. De même, le parc d'instances Spot peut devenir un groupe `c5.large` la prochaine fois. Dans chacune de ces transitions, Amazon EC2 ne donne pas la priorité aux groupes contenant les instances arrêtées le plus tôt, mais définit les priorités uniquement en fonction de la stratégie d'allocation spécifiée. La stratégie `lowestPrice` peut ramener aux pools contenant les instances arrêtées le plus tôt. Par exemple, si des instances sont interrompues dans le pool `c5.large` et que la stratégie `lowestPrice` ramène aux pools `c3.large` ou `c4.large`, les instances arrêtées le plus tôt sont redémarrées pour assurer la capacité cible.

- Pendant qu'une instance Spot est arrêtée, vous pouvez modifier certains de ses attributs, mais pas le type d'instance. Si vous détachez ou supprimez un volume EBS, celui-ci n'est pas attaché lorsque l'instance Spot est démarrée. Si vous détachez le volume racine et qu'Amazon EC2 tente

de démarrer l'instance Spot, l'instance ne peut pas démarrer et Amazon EC2 résilie l'instance arrêtée.

- Vous pouvez résilier une instance Spot pendant qu'elle est arrêtée.
- Si vous annulez une demande d'instance Spot, une flotte EC2 ou un parc d'instances Spot, Amazon EC2 résilie les instances Spot associées qui sont arrêtées.
- Pendant qu'une instance Spot interrompue est arrêtée, seuls les volumes EBS, qui sont préservés, vous sont facturés. Avec une flotte EC2 ou un parc d'instances Spot, si vous avez de nombreuses instances arrêtées, vous pouvez dépasser la limite du nombre de volumes EBS pour votre compte. Pour plus d'informations sur la facturation lorsqu'une instance Spot est interrompue, consultez [Facturation des instances Spot interrompues](#).
- Assurez-vous de bien savoir ce que l'arrêt d'une instance implique. Pour des informations sur ce qui se produit lors de l'arrêt d'une instance, consultez [Différences entre redémarrage, arrêt, mise en veille prolongée et résiliation](#).

Prérequis

Pour arrêter une instance Spot interrompue, les prérequis suivants doivent être réunis :

Type de demande Spot

Type de la demande d'instance spot – doit être persistant. Vous ne pouvez pas spécifier de groupe de lancement dans la demande d'instance Spot.

Type de demande de flotte EC2 ou de parc d'instances Spot – doit être maintenu.

Type de volume racine

Le volume racine doit être un volume EBS, et non un volume de stockage d'instances.

Mettre les instances Spot interrompues en veille prolongée

Vous pouvez préciser qu'Amazon EC2 met en veille prolongée vos instances Spot lorsqu'elles sont interrompues. Pour plus d'informations, consultez [Hibernez votre instance Amazon EC2](#).

Amazon EC2 propose désormais la même expérience de mise en veille prolongée pour les instances Spot que celle actuellement disponible pour les instances à la demande. Cette expérience offre une prise en charge complète, les éléments suivants étant désormais pris en charge pour la mise en veille prolongée des instances Spot :

- [Plus d'AMI prises en charge](#)
- [Plus de familles d'instances prises en charge](#)
- [Mise en veille prolongée à l'initiative de l'utilisateur](#)

Résilier les instances Spot interrompues

Lorsqu'Amazon EC2 interrompt une instance Spot, il résilie l'instance par défaut, sauf si vous spécifiez un autre comportement d'interruption, comme l'arrêt ou la mise en veille prolongée. Pour plus d'informations, consultez [Spécifier le comportement d'interruption](#).

Préparez-vous aux interruptions des instances Spot

La demande d'instances Spot peut varier considérablement d'un instant à l'autre et la disponibilité des instances Spot peut également varier sensiblement selon le nombre d'instances EC2 disponibles qui ne sont pas utilisées. Il est toujours possible que votre instance Spot soit interrompue. Par conséquent, vous devez veiller à ce que votre application soit préparée à une interruption d'instance Spot.

Nous vous recommandons de suivre ces bonnes pratiques afin de vous préparer à subir une interruption d'instance Spot.

- Créez votre demande Spot à l'aide d'un groupe Auto Scaling. Si vos instances Spot sont interrompues, le groupe Auto Scaling lancera automatiquement les instances de remplacement. Pour plus d'informations, consultez [Groupes Auto Scaling avec types d'instance et options d'achat multiples](#) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.
- Veillez à ce que votre instance soit prête pour le lancement dès que la demande est exécutée en utilisant une Amazon Machine Image (AMI) comportant la configuration logicielle requise. Vous pouvez également utiliser les données utilisateur afin d'exécuter les commandes lors du démarrage.
- Les données stockées sur des volumes de stockage d'instance sont perdues lorsque l'instance est arrêtée ou résiliée. Sauvegardez les données importantes qui se trouvent sur les volumes de stockage d'instance vers un stockage plus persistant comme Amazon S3, Amazon EBS ou Amazon DynamoDB.
- Stockez les données importantes régulièrement à un emplacement qui n'est pas touché par la résiliation de l'instance Spot. Par exemple, vous pouvez utiliser Amazon S3, Amazon EBS ou DynamoDB.

- Divisez le travail en petites tâches (à l'aide d'une architecture Grid, Hadoop ou reposant sur les files d'attente) ou utilisez des points de contrôle afin de pouvoir enregistrer votre travail fréquemment.
- Amazon EC2 émet un signal de recommandation de rééquilibrage à l'instance Spot lorsque l'instance présente un risque élevé d'interruption. Vous pouvez vous fier à la recommandation de rééquilibrage pour gérer de manière proactive les interruptions d'instance Spot sans avoir à attendre l'avis d'interruption d'instance Spot à deux minutes. Pour plus d'informations, consultez [Recommandations de rééquilibrage des instances EC2](#).
- Utilisez les avis d'interruption d'instance Spot à deux minutes pour surveiller le statut de vos instances Spot. Pour plus d'informations, consultez [Avis d'interruption d'instance Spot](#).
- Même si nous nous efforçons de vous communiquer ces avertissements dès que possible, il se peut que votre instance Spot soit interrompue avant que les avertissements puissent être mis à disposition. Testez votre application afin de vous assurer qu'elle peut gérer correctement une interruption inattendue d'une instance, même si vous surveillez les signaux de recommandation de rééquilibrage et les avis d'interruption. Pour cela, exécutez l'application en utilisant une instance à la demande, puis résiliez vous-même cette instance à la demande.
- Exécutez une expérience d'injection de pannes contrôlée AWS Fault Injection Service pour tester la façon dont votre application réagit lorsque votre instance Spot est interrompue. Pour plus d'informations, consultez le [Tutorial: Test Spot Instance interruptions using AWS FIS](#) dans le Guide de l'utilisateur AWS Fault Injection Service .

Lancement d'une interruption d'instance Spot

Vous pouvez sélectionner une demande d'instance Spot ou une demande de parc d'instances Spot dans la console Amazon EC2 et lancer une interruption d'instance Spot afin de tester la façon dont les applications de vos instances Spot gèrent les interruptions. Lorsque vous lancez l'interruption d'une instance Spot, Amazon EC2 vous avertit que votre instance Spot sera interrompue dans deux minutes. Puis, au bout de deux minutes, l'instance est interrompue.

Le service sous-jacent qui effectue l'interruption de l'instance Spot est AWS Fault Injection Service (AWS FIS). Pour plus d'informations sur AWS FIS, voir [AWS Fault Injection Service](#).

Note

Les comportements d'interruption sont `terminate`, `stop`, et `hibernate`. Si le comportement d'interruption défini est `hibernate`, lorsque vous lancez l'interruption d'une instance Spot, le processus de mise en veille commence immédiatement.

Le lancement d'une interruption d'instance Spot est pris en charge dans tous les pays Régions AWS sauf en Asie-Pacifique (Jakarta), en Asie-Pacifique (Osaka), en Chine (Pékin), en Chine (Ningxia) et au Moyen-Orient (Émirats arabes unis).

Rubriques

- [Lancer une interruption d'instance Spot](#)
- [Vérifier l'interruption d'instance Spot](#)
- [Quotas](#)

Lancer une interruption d'instance Spot

Vous pouvez utiliser la console EC2 pour lancer rapidement une interruption d'instance Spot. Lorsque vous sélectionnez une demande d'instance Spot, vous pouvez lancer l'interruption d'une instance Spot. Lorsque vous sélectionnez une demande de parc d'instances Spot, vous pouvez lancer l'interruption de plusieurs instances Spot à la fois.

Pour des tests plus avancés visant à tester les interruptions des instances Spot, vous pouvez créer vos propres tests à l'aide de la AWS FIS console.

Pour lancer l'interruption d'une instance Spot dans une demande d'instance Spot à l'aide de la console EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Spot Requests (Demandes Spot).
3. Sélectionnez une demande d'instance Spot, puis sélectionnez Actions, Initiate interruption (Lancer une interruption). Vous ne pouvez pas sélectionner plusieurs demandes d'instance Spot pour lancer une interruption.
4. Dans la boîte de dialogue Initiate Spot Instance interruption (Lancer une interruption d'instance Spot), sous Service access (Accès à un service), utilisez le rôle par défaut ou sélectionnez un

rôle existant. Pour sélectionner un rôle existant, choisissez Utiliser un rôle de service existant, puis, pour Rôle IAM, sélectionnez le rôle à utiliser.

5. Lorsque vous êtes prêt à lancer l'interruption de l'instance Spot, sélectionnez Initiate interruption (Lancer l'interruption).

Pour lancer l'interruption d'une ou de plusieurs instances Spot dans une demande de parc d'instances Spot à l'aide de la console EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Spot Requests (Demandes Spot).
3. Sélectionnez une demande de parc d'instances Spot, puis sélectionnez Actions, Lancer une interruption. Vous ne pouvez pas sélectionner plusieurs demandes de parc d'instances Spot pour lancer une interruption.
4. Dans la boîte de dialogue Spécifier le nombre d'instances Spot, dans le champ Nombre d'instances à interrompre, saisissez le nombre d'instances Spot à interrompre, puis choisissez Confirmer.

 Note

Le nombre ne peut pas dépasser le nombre d'instances ponctuelles du parc ou votre [quota](#) pour le nombre d'instances ponctuelles AWS FIS pouvant être interrompues par expérience.

5. Dans la boîte de dialogue Initiate Spot Instance interruption (Lancer une interruption d'instance Spot), sous Service access (Accès à un service), utilisez le rôle par défaut ou sélectionnez un rôle existant. Pour sélectionner un rôle existant, choisissez Utiliser un rôle de service existant, puis, pour Rôle IAM, sélectionnez le rôle à utiliser.
6. Lorsque vous êtes prêt à lancer l'interruption de l'instance Spot, sélectionnez Initiate interruption (Lancer l'interruption).

Pour créer des expériences plus avancées afin de tester les interruptions d'instances Spot à l'aide de la console AWS FIS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Spot Requests (Demandes Spot).
3. Sélectionnez Actions, Create advanced experiments (Créer des expériences avancées).

La AWS FIS console s'ouvre. Pour plus d'informations, consultez [Didacticiel : tester les interruptions d'instance Spot à l'aide de AWS FIS](#) dans le Guide de l'utilisateur AWS Fault Injection Service .

Vérifier l'interruption d'instance Spot

Après avoir lancé l'interruption, les événements suivants se produisent :

- L'instance Spot reçoit une [recommandation de rééquilibrage d'instance](#).
- Un [avis d'interruption de l'instance Spot](#) est émis deux minutes avant l' AWS FIS interruption de votre instance.
- Après deux minutes, l'instance Spot est interrompue.
- Une instance Spot arrêtée par le AWS FIS reste jusqu'à ce que vous la redémarriez.

Pour vérifier que l'instance a été interrompue après le lancement de l'interruption

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Depuis le panneau de navigation, ouvrez Demandes Spot et Instances dans des onglets ou des fenêtres de navigateur distincts.
3. Pour les demandes Spot, sélectionnez la demande d'instance Spot ou la demande de parc d'instances Spot. L'état initial est fulfilled. Une fois l'instance interrompue, le statut change comme suit, en fonction du comportement d'interruption :
 - terminate – Le statut passe à instance-terminated-by-experiment.
 - stop – Le statut de l'instance passe à marked-for-stop-by-experiment, puis à instance-stopped-by-experiment.
4. Pour Instances, sélectionnez l'instance Spot. L'état initial est Running. Deux minutes après réception de l'avis d'interruption de l'instance Spot, le statut change comme suit, en fonction du comportement d'interruption :
 - stop – Le statut de l'instance passe à Stopping, puis à Stopped.
 - terminate – Le statut de l'instance passe à Shutting-down, puis à Terminated.

Quotas

Vous Compte AWS avez le quota par défaut suivant pour le nombre d'instances ponctuelles AWS FIS pouvant être interrompues par expérience.

Nom	Par défaut	Ajustable	Description
Cible SpotInstances pour aws:ec2:send-spot-instance-interruptions	Chaque Région prise en charge : 5	Oui	Le nombre maximum d'instances ponctuelles que aws:ec2 : send-spot-instance-interruptions peut cibler lorsque vous identifiez des cibles à l'aide de balises, par expérience.

Vous pouvez demander une augmentation de quota. Pour de plus amples informations, veuillez consulter [Demande d'augmentation de quota](#) dans le Guide de l'utilisateur Service Quotas.

Pour afficher tous les quotas pour AWS FIS, ouvrez la [console Service Quotas](#). Dans le panneau de navigation, sélectionnez Services AWS , puis AWS Fault Injection Service. Vous pouvez également consulter tous les [quotas pour AWS Fault Injection Service](#) dans le guide de l'utilisateur AWS Fault Injection Service .

Avis d'interruption d'instance Spot.

Un avis d'interruption d'instance Spot est un avertissement émis deux minutes avant qu'Amazon EC2 arrête ou résilie votre instance Spot. Lorsque vous spécifiez la mise en veille comme comportement d'interruption, vous recevez un avis d'interruption, mais vous ne recevez pas d'avertissement de deux minutes car le processus de mise en veille commence immédiatement.

La meilleure façon pour vous de gérer fluidement les interruptions d'instance Spot consiste à concevoir votre application pour qu'elle soit tolérante aux pannes. Pour ce faire, vous pouvez vous servir des avis d'interruption d'instance Spot. Nous vous recommandons de vérifier ces avis d'interruption toutes les 5 secondes.

Les avis d'interruption sont mis à disposition en tant qu' EventBridge événement et en tant qu'éléments dans les [métadonnées](#) de l'instance Spot. Les avis d'interruption sont créés sur la base du meilleur effort.

EC2 Spot Instance interruption notice

Quand Amazon EC2 va interrompre votre instance Spot, il génère un événement deux minutes avant l'interruption effective (sauf pour la veille prolongée, qui reçoit l'avis d'interruption, mais pas deux minutes à l'avance, car la mise en veille prolongée commence immédiatement). Cet événement peut être détecté par Amazon EventBridge. Pour plus d'informations sur EventBridge les événements, consultez le [guide de EventBridge l'utilisateur Amazon](#). Pour obtenir un exemple détaillé qui vous explique comment créer et utiliser des règles d'événement, consultez [Tirer parti des avis d'interruption d'instance Spot Amazon EC2](#).

Vous trouverez ci-dessous un exemple d'événement pour une interruption d'instance Spot. Les valeurs possibles pour `instance-action` sont `hibernate`, `stop` ou `terminate`.

```
{
  "version": "0",
  "id": "12345678-1234-1234-1234-123456789012",
  "detail-type": "EC2 Spot Instance Interruption Warning",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-2",
  "resources": ["arn:aws:ec2:us-east-2a:instance/i-1234567890abcdef0"],
  "detail": {
    "instance-id": "i-1234567890abcdef0",
    "instance-action": "action"
  }
}
```

Note

Le format ARN de l'événement d'interruption de l'instance Spot est `arn:aws:ec2:availability-zone:instance/instance-id`. Ce format est différent du [format ARN des ressources EC2](#).

instance-action

Si votre instance Spot est marquée comme devant être arrêtée ou résiliée par Amazon EC2, l'élément `instance-action` est présent dans les [métadonnées de l'instance](#). Sinon, il n'est pas présent. Vous pouvez les récupérer `instance-action` à l'aide du service de métadonnées d'instance version 2 (IMDSv2) comme suit.

Utilisez la commande correspondant à votre système d'exploitation.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

L'élément `instance-action` spécifie l'action et l'heure approximative (UTC) à laquelle l'action aura lieu.

L'exemple de sortie suivant indique la date et l'heure auxquelles cette instance sera arrêtée.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

L'exemple de sortie suivant indique la date et l'heure auxquelles cette instance sera résiliée.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Si Amazon EC2 ne s'apprête pas à supprimer ou à arrêter l'instance, ou si vous avez suspendu vous-même l'instance, `instance-action` n'est pas présent dans les métadonnées de l'instance et vous recevez une erreur HTTP 404 lorsque vous tentez de la récupérer.

termination-time

Cet élément est conservé à des fins de compatibilité descendante ; nous vous invitons à utiliser `instance-action` à la place.

Si votre instance Spot est marquée comme devant être résiliée par Amazon EC2 (soit en raison d'une interruption d'instance ponctuelle pour laquelle le comportement d'interruption est défini sur `terminate`, soit en raison de l'annulation d'une demande d'instance ponctuelle persistante), l'élément `termination-time` est présent dans les métadonnées de votre [instance](#). Sinon, il n'est pas présent. Vous pouvez les récupérer à l'aide d'IMDSv2 comme suit.

Utilisez la commande correspondant à votre système d'exploitation.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`  
[ec2-user ~]$ if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo  
    termination_scheduled; fi
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

L'élément `termination-time` indique l'heure approximative en UTC à laquelle l'instance recevra le signal d'arrêt. Voici un exemple de sortie.

```
2015-01-05T18:02:00Z
```

Si Amazon EC2 ne se prépare pas à mettre fin à l'instance (soit parce qu'il n'y a pas d'interruption de l'instance Spot, soit parce que votre comportement d'interruption est défini sur `stop` ou `hibernate`), soit si vous avez résilié l'instance Spot vous-même, l'élément `termination-time` n'est pas présent dans les métadonnées de l'instance (vous recevez donc une erreur HTTP 404) ou contient une valeur qui n'est pas une valeur temporelle.

Si Amazon EC2 ne parvient pas à mettre hors service l'instance, le statut de la demande est défini sur `fulfilled`. La valeur `termination-time` reste dans les métadonnées de l'instance avec l'heure approximative initiale, qui se trouve maintenant dans le passé.

Identifier des instances Spot interrompues

Dans la console, le volet Instances affiche toutes les instances, y compris Instances Spot. Le cycle de vie d'une instance Spot est `spot`. L'état de l'instance d'une instance Spot est soit `stopped`

ou `terminated`, en fonction du comportement d'interruption que vous avez configuré. Pour une instance Spot mise en veille de manière prolongée, l'état de l'instance est `stopped`.

Pour rechercher une instance Spot interrompue à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Appliquez le filtre suivant : Instance lifecycle=spot.
4. Appliquez le filtre Instance state=stopped ou Instance state=terminated en fonction du comportement d'interruption que vous avez configuré.
5. Pour chaque instance Spot, dans l'onglet Détails, sous Détails de l'instance, recherchez le message de transition d'état. Les codes suivants indiquent que l'instance Spot a été interrompue.
 - `Server.SpotInstanceShutdown`
 - `Server.SpotInstanceTermination`
6. Pour plus d'informations sur la raison de l'interruption, consultez le code d'état de la demande Spot. Pour plus d'informations, consultez [the section called "Statut des demandes Spot"](#).

Pour rechercher des instances Spot interrompues à l'aide du AWS CLI

Vous pouvez répertorier les Instances Spot interrompues à l'aide de la commande [describe-instances](#) avec le paramètre `--filters`. Pour répertorier uniquement les ID d'instance dans la sortie, incluez le paramètre `--query`.

Si le comportement d'interruption de l'instance consiste à résilier les instances Spot, utilisez la commande suivante :

```
aws ec2 describe-instances \
  --filters Name=instance-lifecycle,Values=spot Name=instance-state-
  name,Values=terminated Name=state-reason-code,Values=Server.SpotInstanceTermination \
  --query "Reservations[*].Instances[*].InstanceId"
```

Si le comportement d'interruption de l'instance consiste à arrêter les instances Spot, utilisez la commande suivante :

```
aws ec2 describe-instances \
  --filters Name=instance-lifecycle,Values=spot Name=instance-state-
  name,Values=stopped Name=state-reason-code,Values=Server.SpotInstanceShutdown \
```

```
--query "Reservations[*].Instances[*].InstanceId"
```

Déterminer si Amazon EC2 a résilié une instance Spot

Si une instance Spot est résiliée, vous pouvez l'utiliser CloudTrail pour voir si Amazon EC2 l'a résiliée. Dans AWS CloudTrail, le nom de l'évènement BidEvictedEvent indique qu'Amazon EC2 a résilié l'instance Spot.

Pour consulter les BidEvictedEvent événements dans CloudTrail

1. Ouvrez la CloudTrail console à l'[adresse https://console.aws.amazon.com/cloudtrail/](https://console.aws.amazon.com/cloudtrail/).
2. Dans le panneau de navigation, sélectionnez Historique des événements.
3. Dans le menu déroulant du filtre, sélectionnez Nom de l'évènement, puis entrez BidEvictedÉvénement dans le champ de filtre à droite.
4. Choisissez BidEvictedEvent dans la liste qui s'affiche pour en afficher les détails. Sous Enregistrement d'évènement, vous pouvez trouver l'ID d'instance.

Pour plus d'informations sur l'utilisation CloudTrail, consultez [Enregistrez les appels d'API Amazon EC2 à l'aide de AWS CloudTrail](#).

Facturation des instances Spot interrompues

Lors de l'interruption d'une instance Spot, vous êtes facturé pour l'utilisation de l'instance et du volume EBS, et vous pouvez encourir d'autres frais, comme indiqué ci-après.

Utilisation de l'instance

Qui interrompt l'instance Spot	Système d'exploitation	Interrompue au cours de la première heure	Interrompue au cours de toute heure après la première heure
Si vous Arrêtez ou résiliez l'instance Spot	Windows et Linux (à l'exception de SUSE)	Les secondes utilisées sont facturées	Les secondes utilisées sont facturées
	SUSE	L'heure complète est facturée même si	Les heures complètes utilisées sont facturées, et une

Qui interrompt l'instance Spot	Système d'exploitation	Interrompue au cours de la première heure	Interrompue au cours de toute heure après la première heure
		vous n'en avez utilisé qu'une partie	heure complète est facturée pour l'heure partielle interrompue
Si Amazon EC2 interrompt l'instance Spot	Windows et Linux (à l'exception de SUSE)	Aucuns frais.	Les secondes utilisées sont facturées
	SUSE	Aucuns frais.	Les heures complètes utilisées sont facturées, mais l'heure partielle interrompue n'est pas facturée

Utilisation du volume EBS

Pendant qu'une instance Spot interrompue est arrêtée, seuls les volumes EBS, qui sont préservés, vous sont facturés.

Avec une flotte EC2 ou un parc d'instances Spot, si vous avez de nombreuses instances arrêtées, vous pouvez dépasser la limite du nombre de volumes EBS pour votre compte.

Autres frais

Si votre instance Spot en cours d'exécution entraîne des frais pour d'autres services, tels que le transfert de données, les adresses IP élastiques ou l'utilisation d'autres services AWS gérés, leur utilisation vous sera facturée. Ceci indépendamment de la personne qui interrompt l'instance Spot ou du moment où elle a été interrompue. Même si l'utilisation d'une instance Spot ne vous est pas facturée lorsqu'Amazon EC2 interrompt votre instance Spot au cours de la première heure, d'autres frais peuvent vous être facturés.

Pour plus d'informations, veuillez consulter la rubrique [Tarification d'Amazon EC2 à la demande](#).

Score de placement Spot

La fonction de score de placement des Spot peut recommander une AWS région ou une zone de disponibilité en fonction de vos besoins en matière de capacité de Spot. La capacité Spot fluctue et vous ne pouvez pas être sûr d'obtenir toujours la capacité dont vous avez besoin. Un score de placement Spot indique la probabilité qu'une demande Spot soit effectuée avec succès dans une région ou une zone de disponibilité.

Note

Un score de placement Spot ne fournit aucune garantie en termes de capacité disponible ou de risque d'interruption. Un score de placement Spot sert uniquement de recommandation.

Avantages

Vous pouvez utiliser la fonction de score de placement Spot pour les éléments suivants :

- Pour relocaliser et mettre à l'échelle la capacité de calcul Spot dans une autre région, le cas échéant, en réponse à des besoins accrus en capacité ou à une diminution de la capacité disponible dans la région actuelle.
- Pour identifier la zone de disponibilité la plus optimale dans laquelle exécuter les charges de travail de zone de disponibilité unique.
- Pour simuler les besoins futurs en capacité Spot afin de pouvoir choisir une région optimale pour l'expansion de vos charges de travail basées sur Spot.
- Pour trouver une combinaison optimale de types d'instances pour répondre à vos besoins en capacité Spot.

Rubriques

- [Coûts](#)
- [Fonctionnement du score de placement Spot](#)
- [Limites](#)
- [Autorisation IAM requise](#)
- [Calculer un score de placement Spot](#)
- [Exemples de configuration](#)

Coûts

L'utilisation de la fonction de score de placement Spot n'implique aucun coût supplémentaire.

Fonctionnement du score de placement Spot

Lorsque vous utilisez la fonction de score de placement Spot, vous spécifiez d'abord vos exigences de calcul pour vos instances Spot, puis Amazon EC2 renvoie les 10 principales régions ou zones de disponibilité où votre demande Spot est susceptible d'être effectuée avec succès. Chaque région ou zone de disponibilité est évaluée sur une échelle de 1 à 10, 10 indiquant que votre demande Spot est très susceptible de réussir, et 1 indiquant que votre demande Spot n'est pas susceptible de réussir.

Pour utiliser la fonction de score de placement Spot, procédez comme suit :

- [Étape 1 : indiquer vos exigences Spot](#)
- [Étape 2 : filtrer la réponse du score de placement Spot](#)
- [Étape 3 : examiner les recommandations](#)
- [Étape 4 : utiliser les recommandations](#)

Étape 1 : indiquer vos exigences Spot

Tout d'abord, vous spécifiez la capacité Spot cible souhaitée et vos exigences de calcul, comme suit :

1. Spécifiez la capacité Spot cible et éventuellement l'unité de capacité cible.

Vous pouvez spécifier la capacité Spot cible souhaitée en termes de nombre d'instances ou de vCPU, ou en termes de quantité de mémoire en Mio. Pour spécifier la capacité cible en nombre de vCPU ou en quantité de mémoire, vous devez spécifier l'unité de capacité cible en tant que `vcpu` ou `memory-mib`. Sinon, le nombre d'instances est défini par défaut.

En spécifiant votre capacité cible en termes de nombre de vCPU ou de quantité de mémoire, vous pouvez utiliser ces unités lorsque vous comptez la capacité totale. Par exemple, si vous souhaitez utiliser une combinaison d'instances de différentes tailles, vous pouvez spécifier la capacité cible sous forme de nombre total de vCPU. La fonction de score de placement Spot considère ensuite chaque type d'instance de la demande par son nombre de vCPU, puis compte le nombre total de vCPU plutôt que le nombre total d'instances lors de l'augmentation de la capacité cible.

Par exemple, supposons que vous spécifiez une capacité cible totale de 30 vCPU et que votre liste de types d'instance se compose de `c5.xlarge` (4 vCPU), `m5.2xlarge` (8 vCPU) et

r5.large (2 vCPU). Pour atteindre un total de 30 vCPU, vous pouvez combiner 2 vCPU c5.xlarge (2 x 4 vCPU), 2 m5.2xlarge (2 x 8 vCPU) et 3 vCPU r5.large (3 x 2 vCPU).

2. Spécifiez les types d'instance ou les attributs d'instance.

Vous pouvez soit spécifier les types d'instance à utiliser, soit spécifier les attributs d'instance dont vous avez besoin pour vos exigences de calcul, puis laisser Amazon EC2 identifier les types d'instance qui possèdent ces attributs. C'est ce qu'on appelle la sélection de type d'instance basée sur des attributs.

Vous ne pouvez pas spécifier à la fois les types d'instance et les attributs d'instance dans la même demande de score de placement Spot.

Si vous spécifiez des types d'instance, vous devez spécifier au moins trois types d'instance différents, sinon Amazon EC2 renvoie un score de placement Spot faible. De même, si vous spécifiez des attributs d'instance, ils doivent être résolus à au moins trois types d'instance différents.

Pour obtenir des exemples de différentes manières de spécifier vos exigences Spot, consultez [Exemples de configuration](#).

Étape 2 : filtrer la réponse du score de placement Spot

Amazon EC2 calcule le score de placement Spot pour chaque région ou zone de disponibilité, et renvoie les 10 principales régions ou zones de disponibilité où votre demande Spot est susceptible d'aboutir. Le procédé par défaut consiste à renvoyer une liste de régions évaluées. Si vous envisagez de lancer toute votre capacité Spot dans une seule zone de disponibilité, il est utile de demander une liste de zones de disponibilité évaluées.

Vous pouvez spécifier un filtre de région pour affiner les régions qui seront renvoyées dans la réponse.

Vous pouvez combiner le filtre Région et une demande de zones de disponibilité évaluées. De cette façon, les zones de disponibilité évaluées sont limitées aux régions filtrées. Pour trouver la zone de disponibilité la mieux notée dans une région, spécifiez uniquement cette région, et la réponse renvoie une liste notée de toutes les zones de disponibilité de cette région.

Étape 3 : examiner les recommandations

Le score de placement Spot pour chaque région ou zone de disponibilité est calculé en fonction de la capacité cible, de la composition des types d'instance, des tendances historiques et actuelles de

l'utilisation Spot et de l'heure de la demande. Étant donné que la capacité Spot fluctue constamment, la même demande de score de placement Spot peut générer des scores différents lorsqu'elle est calculée à des moments différents.

Les régions et les zones de disponibilité sont évaluées sur une échelle de 1 à 10. Un score de 10 indique que votre demande Spot est très susceptible, mais non garantie, d'aboutir. Un score de 1 indique que votre demande Spot a peu de chances d'aboutir. Le même score peut être renvoyé pour différentes régions ou zones de disponibilité.

Si des scores faibles sont renvoyés, vous pouvez modifier vos exigences de calcul et recalculer le score. Vous pouvez également demander des recommandations de score de placement Spot pour les mêmes exigences de calcul à différents moments de la journée.

Étape 4 : utiliser les recommandations

Un score de placement Spot n'est pertinent que si votre demande Spot a exactement la même configuration que celle du score de placement Spot (capacité cible, unité de capacité cible, types d'instance ou attributs d'instance) et est configurée pour utiliser la stratégie d'allocation `capacity-optimized`. Sinon, la probabilité d'obtenir une capacité Spot disponible ne sera pas alignée sur le score.

Bien qu'un score de placement Spot serve de directive et qu'aucun score ne garantit que votre demande Spot sera entièrement ou partiellement satisfaite, vous pouvez utiliser les informations suivantes pour obtenir les meilleurs résultats :

- Utiliser la même configuration : le score de placement Spot n'est pertinent que si la configuration de demande Spot (capacité cible, unité de capacité cible, types d'instance ou attributs d'instance) dans votre groupe Auto Scaling, flotte EC2 ou parc d'instances Spot est identique à celle que vous avez saisie pour obtenir le score de placement Spot.

Si vous avez utilisé la sélection de type d'instance basée sur des attributs dans votre demande de score de placement Spot, vous pouvez utiliser la sélection de type d'instance basée sur des attributs pour configurer votre groupe Auto Scaling, flotte EC2 ou parc d'instances Spot. Pour plus d'informations, consultez [Création d'un groupe Auto Scaling à l'aide de la sélection de type d'instance basée sur des attributs](#), [Sélection de type d'instance basée sur des attributs pour la flotte EC2](#) et [Sélection de type d'instance basée sur des attributs pour un parc d'instances Spot](#).

Note

Si vous avez spécifié votre capacité cible en termes de nombre de vCPU ou de quantité de mémoire, et que vous avez spécifié des types d'instance dans votre configuration de score de placement Spot, notez que vous ne pouvez actuellement pas créer cette configuration dans votre groupe Auto Scaling, flotte EC2 ou parc d'instances Spot. À la place, vous devez définir manuellement la pondération de l'instance à l'aide du paramètre `WeightedCapacity`.

- Utiliser la stratégie d'allocation **capacity-optimized** : tout score suppose que votre demande de flotte sera configurée pour utiliser toutes les zones de disponibilité (pour demander de la capacité dans toutes les régions) ou une seule zone de disponibilité (si vous demandez une capacité dans une zone de disponibilité) et la stratégie d'allocation Spot `capacity-optimized` pour que votre demande de capacité Spot aboutisse. Si vous utilisez d'autres stratégies d'allocation, telles que `lowest-price`, la probabilité d'obtenir une capacité Spot disponible ne sera pas alignée sur le score.
- Agir immédiatement après l'obtention du score : la recommandation de score de placement Spot reflète la capacité Spot disponible au moment de la demande, et la même configuration peut générer des scores différents lorsqu'elle est calculée à des moments différents en raison des fluctuations de capacité Spot. Bien qu'un score de 10 signifie que votre demande de capacité Spot est très susceptible, mais non garantie, d'aboutir, pour obtenir de meilleurs résultats, nous vous recommandons d'agir immédiatement après l'obtention du score. Nous vous recommandons également d'obtenir un nouveau score chaque fois que vous tentez une demande de capacité.

Limites

- Limite de capacité cible : la limite de capacité cible de votre score de placement Spot est basée sur votre récente utilisation Spot, tout en tenant compte de la croissance potentielle de l'utilisation. Si vous n'avez pas récemment utilisé Spot, nous vous fournissons une limite par défaut faible alignée sur votre limite de demande Spot.
- Limite des configurations de demande : nous pouvons limiter le nombre de nouvelles configurations de demande sur une période de 24 heures si nous détectons des modèles non associés à l'utilisation prévue de la fonction de score de placement Spot. Si vous atteignez la limite, vous pouvez réessayer les configurations de demande que vous avez déjà utilisées, mais vous ne pouvez pas spécifier de nouvelles configurations de demande avant les prochaines 24 heures.

- Nombre minimum de types d'instance : si vous spécifiez des types d'instance, vous devez spécifier au moins trois types d'instance différents, sinon Amazon EC2 renverra un score de placement Spot faible. De même, si vous spécifiez des attributs d'instance, ils doivent être résolus à au moins trois types d'instance différents. Les types d'instance sont considérés comme différents s'ils portent un nom différent. Par exemple, m5.8xlarge, m5a.8xlarge et m5.12xlarge sont tous considérés comme différents.

Autorisation IAM requise

Par défaut, les identités IAM (utilisateurs, rôles ou groupes) ne sont pas autorisées à utiliser la fonction de score de placement Spot. Pour autoriser les identités IAM à utiliser la fonction de score de placement Spot, vous devez créer une politique IAM qui accorde l'autorisation d'utiliser l'action d'API EC2 `ec2:GetSpotPlacementScores`. Ensuite, vous attachez la politique aux identités IAM qui nécessitent l'autorisation.

Voici un exemple de politique IAM qui accorde l'autorisation d'utiliser l'action d'API EC2 `ec2:GetSpotPlacementScores`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:GetSpotPlacementScores",
      "Resource": "*"
    }
  ]
}
```

Pour en savoir plus sur la modification d'une politique IAM, consultez [Modification de politiques IAM](#) dans le Guide de l'utilisateur IAM.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :
 - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.
 - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Calculer un score de placement Spot

Vous pouvez calculer un score de placement Spot à l'aide de la console Amazon EC2 ou de la AWS CLI.

Rubriques

- [Calculer un score de placement Spot en spécifiant des attributs d'instance \(console\)](#)
- [Calculer un score de placement Spot en spécifiant des types d'instance \(console\)](#)
- [Calculer le score de placement Spot \(AWS CLI\)](#)

Calculer un score de placement Spot en spécifiant des attributs d'instance (console)

Pour calculer un score de placement Spot en spécifiant des attributs d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Choisissez Spot placement score (Score de placement Spot).
4. Choisissez Enter requirements (Saisir les exigences).
5. Pour Target capacity (Capacité cible), saisissez la capacité souhaitée en fonction du nombre d'instances ou de vCPU, ou de la quantité de mémoire (Mio).
6. Pour Instance type requirements (Exigences du type d'instance), pour spécifier vos exigences de calcul et permettre à Amazon EC2 d'identifier les types d'instances optimaux selon ces exigences, choisissez Specify instance attributes that match your compute requirements (Spécifier les attributs d'instance qui correspondent à vos exigences de calcul).

7. Pour vCPU, saisissez les nombres minimum et maximum de vCPU souhaités. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.
8. Pour Memory (GiB) (Mémoire (Go)), saisissez la quantité minimale et maximale de mémoire souhaitée. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.
9. Pour CPU architecture (Architecture du processeur), sélectionnez l'architecture d'instance requise.
10. (Facultatif) Pour Additional instance attributes (Attributs d'instance supplémentaires), vous pouvez éventuellement spécifier un ou plusieurs attributs pour exprimer vos exigences de calcul plus en détail. Chaque attribut supplémentaire ajoute une contrainte supplémentaire à votre demande. Vous pouvez omettre les attributs supplémentaires. Lorsque ces attributs sont omis, les valeurs par défaut sont utilisées. Pour obtenir une description de chaque attribut et de leurs valeurs par défaut, consultez [get-spot-placement-scores](#) dans la Référence des commandes en ligne d'Amazon EC2.
11. (Facultatif) Pour afficher les types d'instance avec vos attributs spécifiés, développez Preview matching instance types (Aperçu des types d'instance correspondants). Pour empêcher des types d'instances d'être utilisés dans l'évaluation du placement, sélectionnez les instances, puis choisissez Exclude selected instance types (Exclure les types d'instances sélectionnés).
12. Choisissez Load placement scores (Charger les scores de placement) et vérifiez les résultats.
13. (Facultatif) Pour afficher le score de placement Spot pour des régions spécifiques, pour Regions to evaluate (Régions à évaluer), sélectionnez les régions à évaluer, puis choisissez Calculate placement scores (Calculer les scores de placement).
14. (Facultatif) Pour afficher le score de placement Spot pour les zones de disponibilité dans les régions affichées, cochez la case Provide placement scores per Availability Zone (Fournir des scores de placement par zone de disponibilité). Une liste de zones de disponibilité évaluées est utile si vous souhaitez lancer toute votre capacité Spot dans une seule zone de disponibilité.
15. (Facultatif) Pour modifier vos exigences de calcul et obtenir un nouveau score de placement, choisissez Edit (Modifier), effectuez les ajustements nécessaires, puis choisissez Calculate placement scores (Calculer les scores de placement).

Calculer un score de placement Spot en spécifiant des types d'instance (console)

Pour calculer un score de placement Spot en spécifiant des types d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Choisissez Spot placement score (Score de placement Spot).
4. Choisissez Enter requirements (Saisir les exigences).
5. Pour Target capacity (Capacité cible), saisissez la capacité souhaitée en fonction du nombre d'instances ou de vCPU, ou de la quantité de mémoire (Mio).
6. Pour Instance type requirements (Exigences de type d'instance), afin de spécifier les types d'instance à utiliser, choisissez Manually select instance types (Sélection manuelle des types d'instance).
7. Choisissez Select instance types (Sélectionner les types d'instance), sélectionnez les types d'instance à utiliser, puis choisissez Select (Sélectionner). Pour trouver rapidement des types d'instance, vous pouvez utiliser la barre de filtre afin de filtrer les types d'instance selon différentes propriétés.
8. Choisissez Load placement scores (Charger les scores de placement) et vérifiez les résultats.
9. (Facultatif) Pour afficher le score de placement Spot pour des régions spécifiques, pour Regions to evaluate (Régions à évaluer), sélectionnez les régions à évaluer, puis choisissez Calculate placement scores (Calculer les scores de placement).
10. (Facultatif) Pour afficher le score de placement Spot pour les zones de disponibilité dans les régions affichées, cochez la case Provide placement scores per Availability Zone (Fournir des scores de placement par zone de disponibilité). Une liste de zones de disponibilité évaluées est utile si vous souhaitez lancer toute votre capacité Spot dans une seule zone de disponibilité.
11. (Facultatif) Pour modifier la liste des types d'instance et obtenir un nouveau score de placement, choisissez Edit (Modifier), effectuez les ajustements nécessaires, puis choisissez Calculate placement scores (Calculer les scores de placement).

Calculer le score de placement Spot (AWS CLI)

Pour calculer le score de placement Spot

1. (Facultatif) Pour générer tous les paramètres possibles qui peuvent être spécifiés pour la configuration du score de placement Spot, utilisez la commande [get-spot-placement-scores](#) et le paramètre `--generate-cli-skeleton`.

```
aws ec2 get-spot-placement-scores \  
  --region us-east-1 \  
  --generate-cli-skeleton
```

Sortie attendue

```
{  
  "InstanceTypes": [  
    ""  
  ],  
  "TargetCapacity": 0,  
  "TargetCapacityUnitType": "vcpu",  
  "SingleAvailabilityZone": true,  
  "RegionNames": [  
    ""  
  ],  
  "InstanceRequirementsWithMetadata": {  
    "ArchitectureTypes": [  
      "x86_64_mac"  
    ],  
    "VirtualizationTypes": [  
      "hvm"  
    ],  
    "InstanceRequirements": {  
      "VCpuCount": {  
        "Min": 0,  
        "Max": 0  
      },  
      "MemoryMiB": {  
        "Min": 0,  
        "Max": 0  
      },  
      "CpuManufacturers": [  
        "amd"  
      ]  
    }  
  }  
}
```

```
    ],
    "MemoryGiBPerVCpu": {
      "Min": 0.0,
      "Max": 0.0
    },
  ],
  "ExcludedInstanceTypes": [
    ""
  ],
  ],
  "InstanceGenerations": [
    "previous"
  ],
  ],
  "SpotMaxPricePercentageOverLowestPrice": 0,
  "OnDemandMaxPricePercentageOverLowestPrice": 0,
  "BareMetal": "excluded",
  "BurstablePerformance": "excluded",
  "RequireHibernateSupport": true,
  "NetworkInterfaceCount": {
    "Min": 0,
    "Max": 0
  },
  ],
  "LocalStorage": "included",
  "LocalStorageTypes": [
    "hdd"
  ],
  ],
  "TotalLocalStorageGB": {
    "Min": 0.0,
    "Max": 0.0
  },
  ],
  "BaselineEbsBandwidthMbps": {
    "Min": 0,
    "Max": 0
  },
  ],
  "AcceleratorTypes": [
    "fpga"
  ],
  ],
  "AcceleratorCount": {
    "Min": 0,
    "Max": 0
  },
  ],
  "AcceleratorManufacturers": [
    "amd"
  ],
  ],
  "AcceleratorNames": [
    "vu9p"
```

```
    ],
    "AcceleratorTotalMemoryMiB": {
      "Min": 0,
      "Max": 0
    }
  },
  "DryRun": true,
  "MaxResults": 0,
  "NextToken": ""
}
```

2. Créez un fichier de configuration JSON à l'aide de la sortie de l'étape précédente et configurez-le comme suit :
 - a. Pour `TargetCapacity`, saisissez la capacité Spot souhaitée en fonction du nombre d'instances ou de vCPU, ou de la quantité de mémoire (Mio).
 - b. Pour `TargetCapacityUnitType`, saisissez l'unité correspondant à la capacité cible. Si vous omettez ce paramètre, `units` est utilisé par défaut.

Valeurs valides : `units` (qui se traduit par le nombre d'instances) | `vcpu` | `memory-mib`

- c. Pour `SingleAvailabilityZone`, spécifiez `true` pour une réponse qui renvoie une liste de zones de disponibilité évaluées. Une liste de zones de disponibilité évaluées est utile si vous souhaitez lancer toute votre capacité Spot dans une seule zone de disponibilité. Si vous omettez ce paramètre, `false` est utilisé par défaut et la réponse renvoie une liste des régions notées.
 - d. (Facultatif) Pour `RegionNames`, spécifiez les régions à utiliser comme filtre. Vous devez spécifier le code de région, par exemple, `us-east-1`.

Avec un filtre de région, la réponse renvoie uniquement les régions que vous spécifiez. Si vous avez spécifié `true` pour `SingleAvailabilityZone`, la réponse renvoie uniquement les zones de disponibilité dans les régions spécifiées.

- e. Vous pouvez inclure `InstanceTypes` ou `InstanceRequirements`, mais pas les deux dans la même configuration.

Spécifiez l'un des éléments suivants dans votre configuration JSON :

- Pour spécifier une liste de types d'instances, spécifiez les types d'instances dans le paramètre `InstanceTypes`. Spécifiez au moins trois types d'instance différents. Si

vous ne spécifiez qu'un ou deux types d'instance, le score de placement Spot renvoie un score faible. Pour accéder à la liste des types d'instance, consultez [Types d'instances Amazon EC2](#).

- Pour spécifier les attributs d'instance afin qu'Amazon EC2 identifie les types d'instance qui correspondent à ces attributs, spécifiez les attributs situés dans la structure InstanceRequirements.

Vous devez fournir des valeurs pour VCpuCount, MemoryMiB et CpuManufacturers. Vous pouvez omettre les autres attributs. Lorsqu'ils sont omis, les valeurs par défaut sont utilisées. Pour obtenir une description de chaque attribut et de leurs valeurs par défaut, consultez [get-spot-placement-scores](#) dans la Référence des commandes en ligne d'Amazon EC2.

Pour obtenir des exemples de configuration, consultez [Exemples de configuration](#).

3. Pour obtenir le score de placement Spot correspondant aux exigences que vous avez spécifiées dans le fichier JSON, utilisez la commande [get-spot-placement-scores](#) et spécifiez le nom et le chemin d'accès à votre fichier JSON à l'aide du paramètre `--cli-input-json`.

```
aws ec2 get-spot-placement-scores \
  --region us-east-1 \
  --cli-input-json file://file_name.json
```

Exemple de sortie si SingleAvailabilityZone est défini sur false ou omis (en cas d'omission, false est utilisé par défaut) : une liste de régions notées est renvoyée

```
"SpotPlacementScores": [
  {
    "Region": "us-east-1",
    "Score": 7
  },
  {
    "Region": "us-west-1",
    "Score": 5
  },
  ...
]
```

Exemple de sortie si SingleAvailabilityZone est défini sur true : une liste notée des zones de disponibilité est renvoyée

```
"SpotPlacementScores": [  
  {  
    "Region": "us-east-1",  
    "AvailabilityZoneId": "use1-az1"  
    "Score": 8  
  },  
  {  
    "Region": "us-east-1",  
    "AvailabilityZoneId": "usw2-az3"  
    "Score": 6  
  },  
  ...  
]
```

Exemples de configuration

Lorsque vous utilisez le AWS CLI, vous pouvez utiliser les exemples de configuration suivants.

Exemples de configuration

- [Exemple : spécifier les types d'instance et la capacité cible](#)
- [Exemple : spécifier les types d'instance et la capacité cible en termes de mémoire](#)
- [Exemple : spécifier des attributs pour la sélection du type d'instance basée sur des attributs](#)
- [Exemple : spécifier des attributs pour la sélection du type d'instance basée sur des attributs et renvoyer une liste de zones de disponibilité évaluées](#)

Exemple : spécifier les types d'instance et la capacité cible

L'exemple de configuration suivant spécifie trois types d'instance différents et une capacité Spot cible de 500 instances Spot.

```
{  
  "InstanceTypes": [  
    "m5.4xlarge",  
    "r5.2xlarge",  
    "m4.4xlarge"  
  ],  
  "TargetCapacity": 500  
}
```

Exemple : spécifier les types d'instance et la capacité cible en termes de mémoire

L'exemple de configuration suivant spécifie trois types d'instance différents et une capacité Spot cible de 500 000 Mio de mémoire, où le nombre d'instances Spot à lancer doit fournir un total de 500 000 Mio de mémoire.

```
{
  "InstanceTypes": [
    "m5.4xlarge",
    "r5.2xlarge",
    "m4.4xlarge"
  ],
  "TargetCapacity": 500000,
  "TargetCapacityUnitType": "memory-mib"
}
```

Exemple : spécifier des attributs pour la sélection du type d'instance basée sur des attributs

L'exemple de configuration suivant est configuré pour la sélection du type d'instance basé sur des attributs et est suivi d'une explication textuelle.

```
{
  "TargetCapacity": 5000,
  "TargetCapacityUnitType": "vcpu",
  "InstanceRequirementsWithMetadata": {
    "ArchitectureTypes": ["arm64"],
    "VirtualizationTypes": ["hvm"],
    "InstanceRequirements": {
      "VCpuCount": {
        "Min": 1,
        "Max": 12
      },
      "MemoryMiB": {
        "Min": 512
      }
    }
  }
}
```

InstanceRequirementsWithMetadata

Pour utiliser la sélection du type d'instance basée sur les attributs, vous devez inclure la structure `InstanceRequirementsWithMetadata` dans votre configuration et spécifier les attributs souhaités pour les instances Spot.

Dans l'exemple précédent, les attributs d'instance obligatoires suivants sont spécifiés :

- `ArchitectureTypes` – le type d'architecture des types d'instance doit être `arm64`.
- `VirtualizationTypes` – le type de virtualisation des types d'instance doit être `hvm`.
- `VCpuCount` : les types d'instance doivent comporter au minimum un et au maximum 12 vCPU.
- `MemoryMiB` : les types d'instance doivent avoir un minimum de 512 Mio de mémoire. En omettant le paramètre `Max`, vous indiquez qu'il n'y a pas de limite maximale.

Notez qu'il existe plusieurs autres attributs facultatifs que vous pouvez spécifier. Pour obtenir la liste des attributs, consultez [get-spot-placement-scores](#) dans la Référence des commandes en ligne d'Amazon EC2.

TargetCapacityUnitType

Le paramètre `TargetCapacityUnitType` spécifie l'unité de la capacité cible. Dans cet exemple, la capacité cible est `5000` et le type d'unité de capacité cible est `vcpu`, qui spécifient ensemble une capacité cible souhaitée de 5 000 vCPU, où le nombre d'instances Spot à lancer doit fournir un total de 5 000 vCPU.

Exemple : spécifier des attributs pour la sélection du type d'instance basée sur des attributs et renvoyer une liste de zones de disponibilité évaluées

L'exemple de configuration suivant est configuré pour la sélection du type d'instance basée sur des attributs. En spécifiant `"SingleAvailabilityZone": true`, la réponse renverra une liste des zones de disponibilité évaluées.

```
{
  "TargetCapacity": 1000,
  "TargetCapacityUnitType": "vcpu",
  "SingleAvailabilityZone": true,
  "InstanceRequirementsWithMetadata": {
    "ArchitectureTypes": ["arm64"],
    "VirtualizationTypes": ["hvm"],
    "InstanceRequirements": {
      "VCpuCount": {
```

```
        "Min": 1,  
        "Max": 12  
    },  
    "MemoryMiB": {  
        "Min": 512  
    }  
}  
}
```

Flux de données des instances Spot

Pour vous aider à comprendre les frais associés à vos instances Spot, Amazon EC2 fournit un flux de données qui décrit votre utilisation des instances Spot et leur tarification. Ce flux de données est envoyé vers un compartiment Amazon S3 que vous spécifiez lorsque vous vous abonnez au flux de données.

Les fichiers de flux de données arrivent généralement dans votre compartiment toutes les heures et chaque heure d'utilisation est généralement couverte dans un seul fichier de données. Ces fichiers sont compressés (gzip) avant qu'ils ne soient livrés à votre compartiment. Amazon EC2 peut inscrire les données dans plusieurs fichiers pour une heure spécifique d'utilisation lorsque les fichiers sont volumineux (par exemple, si le contenu du fichier pour cette heure dépasse les 50 Mo avant compression).

Note

Vous ne pouvez créer qu'un seul flux de données d'instance Spot par Compte AWS. Si vous n'avez aucune instance Spot en cours d'exécution à une certaine heure, vous ne recevez pas de fichier de flux de données pour cette heure.

Le flux de données des instances Spot est pris en charge dans toutes les AWS régions à l'exception de la Chine (Pékin), de la Chine AWS GovCloud (Ningxia), (États-Unis) et des [régions qui sont désactivées par défaut](#).

Table des matières

- [Nom et format du fichier de flux de données](#)
- [Conditions requises pour le compartiment Amazon S3](#)
- [S'abonner à votre flux de données d'instance Spot](#)

- [Décrire votre flux de données d'instance Spot](#)
- [Afficher les données dans votre flux de données](#)
- [Supprimer votre flux de données d'instance Spot](#)

Nom et format du fichier de flux de données

Le nom du fichier de flux de données d'instance Spot utilise le format suivant (avec la date et l'heure au format UTC) :

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Par exemple, si le nom de votre compartiment est **my-bucket-name** et que votre préfixe est **my-prefix**, vos noms de fichier ont le format suivant :

```
my-bucket-name.s3.amazonaws.com/my-prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Pour plus d'informations sur les noms de compartiment, veuillez consulter la rubrique [Règles de dénomination de compartiment](#) dans le Guide de l'utilisateur Amazon S3.

Les fichiers de flux de données d'instance Spot sont délimités par des tabulations. Chaque ligne du fichier de données correspond à une heure d'instance et contient les champs répertoriés dans le tableau suivant.

Champ	Description
Timestamp	Horodatage utilisé pour déterminer le prix facturé pour cette utilisation d'instance.
UsageType	Type d'utilisation et type d'instance associés à la facturation. Pour <code>m1.small</code> Instances Spot, ce champ est défini sur <code>SpotUsage</code> . Pour tous les autres types d'instance, ce champ est défini sur <code>SpotUsage: {instance-type}</code> . Par exemple, <code>SpotUsage:c1.medium</code> .
Operation	

Champ	Description
	Le produit faisant l'objet d'une facturation. Pour les Instances Spot Linux, ce champ est défini sur <code>RunInstances</code> . Pour les Instances Spot Windows, ce champ est défini sur <code>RunInstances:0002</code> . L'utilisation des instances Spot est regroupée par zone de disponibilité.
InstanceID	L'ID de l'instance Spot qui a généré cette utilisation d'instance.
MyBidID	L'ID de la demande d'instance Spot qui a généré cette utilisation d'instance.
MyMaxPrice	Prix maximum spécifié pour cette demande Spot.
MarketPrice	Prix Spot au moment spécifié dans le champ <code>Timestamp</code> .
Charge	Prix facturé pour cette utilisation d'instance.
Version	Version du flux de données. La version disponible est la version 1.0.

Conditions requises pour le compartiment Amazon S3

Lorsque vous vous abonnez au flux de données, vous devez spécifier un compartiment Amazon S3 afin de stocker les fichiers de flux de données.

Avant de choisir un compartiment Amazon S3 pour le flux de données, tenez compte des points suivants :

- Vous devez bénéficier d'une autorisation `FULL_CONTROL` sur le compartiment. Si vous êtes le propriétaire du compartiment, vous disposez de cette autorisation par défaut. Dans le cas contraire, le propriétaire du bucket doit vous accorder Compte AWS cette autorisation.
- Lorsque vous vous abonnez à un flux de données, ces autorisations sont utilisées pour mettre à jour l'ACL du bucket afin d'`FULL_CONTROL` autoriser le compte du flux de AWS données. Le compte AWS de flux de données écrit des fichiers de flux de données dans le compartiment. Si votre compte ne dispose pas des autorisations nécessaires, les fichiers de flux de données ne

peuvent pas être écrits dans le compartiment. Pour plus d'informations, consultez la section [Logs envoyés à Amazon S3](#) dans le guide de l'utilisateur Amazon CloudWatch Logs.

 Note

Si vous mettez à jour l'ACL et supprimez les autorisations pour le compte de flux de AWS données, les fichiers de flux de données ne peuvent pas être écrits dans le bucket. Vous devez vous réabonner au flux de données pour recevoir les fichiers de flux de données.

- Chaque fichier de flux de données a son propre ACL (distinct de celui du compartiment). Le propriétaire du compartiment bénéficie de l'autorisation FULL_CONTROL pour les fichiers de données. Le compte du flux de AWS données dispose d'autorisations de lecture et d'écriture.
- Si vous avez appliqué des ACL désactivées à vos compartiments, ajoutez une stratégie de compartiment qui permet aux utilisateurs ayant un contrôle total d'écrire dans le compartiment. Pour plus d'informations, veuillez consulter la rubrique [Vérifiez et mettez à jour les stratégies de compartiment](#).
- Si vous supprimez votre abonnement au flux de données, Amazon EC2 ne supprime pas les autorisations de lecture et d'écriture du compte de flux de AWS données, que ce soit sur le compartiment ou sur les fichiers de données. Vous devez supprimer ces autorisations vous-même.
- Vous devez utiliser une clé gérée par le client si vous cryptez votre compartiment Amazon S3 à l'aide d'un chiffrement côté serveur avec une AWS KMS clé stockée dans AWS Key Management Service (SSE-KMS). Pour plus d'informations, consultez la section [Chiffrement du compartiment Amazon S3 côté serveur dans le](#) guide de l'utilisateur Amazon CloudWatch Logs.

 Note

Pour le flux de données des instances Spot, la ressource qui génère les fichiers S3 n'est plus Amazon CloudWatch Logs. Vous devez donc supprimer la section `aws:SourceArn` de la politique d'autorisation du compartiment S3 et de la politique KMS.

S'abonner à votre flux de données d'instance Spot

Pour vous abonner à votre flux de données, utilisez la commande [create-Spot-datafeed-subscription](#).

```
aws ec2 create-spot-datafeed-subscription \  
  --bucket my-bucket-name \  
  --
```

```
[--prefix my-prefix]
```

Exemple de sortie

```
{
  "SpotDatafeedSubscription": {
    "OwnerId": "111122223333",
    "Bucket": "my-bucket-name",
    "Prefix": "my-prefix",
    "State": "Active"
  }
}
```

Décrire votre flux de données d'instance Spot

Pour décrire votre abonnement au flux de données, utilisez la commande [describe-spot-datafeed-subscription](#) .

```
aws ec2 describe-spot-datafeed-subscription
```

Exemple de sortie

```
{
  "SpotDatafeedSubscription": {
    "OwnerId": "123456789012",
    "Prefix": "spotdata",
    "Bucket": "my-s3-bucket",
    "State": "Active"
  }
}
```

Afficher les données dans votre flux de données

Dans le AWS Management Console, ouvrez AWS CloudShell. Utilisez la commande de [s3 sync](#) suivante pour obtenir les fichiers .gz du compartiment S3 pour votre flux de données et stockez-les dans le dossier que vous spécifiez.

```
aws s3 sync s3://my-s3-bucket ./data-feed
```

Pour afficher le contenu d'un fichier .gz, accédez au dossier dans lequel vous avez stocké le contenu du compartiment S3.

```
cd data-feed
```

Utilisez la commande `ls` pour afficher les noms des fichiers. Utilisez la commande `zcat` avec le nom du fichier pour afficher le contenu du fichier compressé. Voici un exemple de commande.

```
zcat 111122223333.2023-12-09-07.001.b959dbc6.gz
```

Voici un exemple de sortie.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium RunInstances:SV050
i-0c3e0c0b046e050df sir-pwq6nmfp 0.0510000000 USD 0.0142000000 USD
0.0142000000 USD 1
```

Supprimer votre flux de données d'instance Spot

Pour supprimer votre flux de données, utilisez la commande [delete-spot-datafeed-subscription](#).

```
aws ec2 delete-spot-datafeed-subscription
```

Quotas d'instances Spot

Il existe des quotas pour le nombre d'instances Spot en cours d'exécution et les demandes d'instances Spot en attente par Compte AWS et par région. Une fois qu'une demande d'instance Spot en attente est traitée, elle n'est plus prise en compte dans le quota, car l'instance en cours d'exécution est prise en compte dans le quota.

Les quotas des instances Spot sont maintenant gérés en fonction du nombre de CPU virtuels (vCPU) que vos instances Spot en cours d'exécution utilisent ou utiliseront en attendant le traitement des demandes d'instances Spot ouvertes. Si vous résiliez vos instances Spot, mais que vous n'annulez pas les demandes d'instances Spot, ces dernières sont comptabilisées par rapport au quota vCPU de vos instances Spot jusqu'à ce qu'Amazon EC2 détecte les résiliations et clôture les demandes.

Nous proposons les types de quotas suivants pour les instances Spot :

- Toutes les demandes d'instance Spot DL

- Toutes les demandes d'instance Spot F
- Toutes les demandes d'instance Spot G et VT
- Toutes les demandes d'instance Spot Inf
- Toutes les demandes d'instance Spot P
- Toutes les demandes d'instance Spot standard (A, C, D, H, I, M, R, T, Z)
- Toutes les demandes d'instance Spot Trn
- Toutes les demandes d'instance Spot X

Chaque type de quota spécifie le nombre maximum de vCPU pour une ou plusieurs familles d'instances. Pour plus d'informations sur les différentes familles, générations et tailles d'instances, consultez [Types d'instance Amazon EC2](#).

Vous pouvez lancer toute combinaison de types d'instance qui répond à l'évolution de vos besoins en termes d'applications. Par exemple, avec un quota Toutes les demandes d'instances Spot standard de 256 vCPU, vous pouvez demander 32 instances Spot m5.2xlarge (32 x 8 vCPU) ou 16 instances Spot c5.4xlarge (16 x 16 vCPU).

Tâches

- [Surveiller les quotas et l'utilisation des instances Spot](#)
- [Demander une augmentation de quota](#)

Surveiller les quotas et l'utilisation des instances Spot

Vous pouvez afficher et gérer les quotas de vos instances Spot à l'aide des éléments suivants :

- La [page Quotas de service](#) Amazon EC2 dans la console Service Quotas
- Le [get-service-quota](#) AWS CLI

Pour plus d'informations, reportez-vous à la section « [Affichage Quotas de service Amazon EC2 des quotas de service](#) » dans le Guide de l'utilisateur des quotas de service.

Grâce à l'intégration CloudWatch des métriques Amazon, vous pouvez surveiller l'utilisation d'EC2 par rapport à vos quotas. Vous pouvez également configurer des alarmes pour vous avertir lorsque vous approchez des quotas. Pour plus d'informations, consultez la section [Quotas de service et CloudWatch alarmes Amazon](#) dans le guide de l'utilisateur des quotas de service. .

Demander une augmentation de quota

Même si Amazon EC2 augmente automatiquement vos quotas d'instances Spot en fonction de votre utilisation, vous pouvez demander une augmentation de quota si nécessaire. Par exemple, si vous avez l'intention de lancer plus d'instances Spot que celles autorisées par votre quota actuel, vous pouvez demander une augmentation de quota. Vous pouvez aussi demander une augmentation de quota si vous soumettez une demande d'instance Spot et que vous recevez l'erreur `Max spot instance count exceeded`. Pour demander une augmentation de quota, utilisez la console Service Quotas, comme décrit dans [Quotas de service Amazon EC2](#).

Instances de performance à capacité extensible

Les types d'instances T sont des [instances à capacité extensible](#). Si vous lancez vos instances Spot à l'aide d'un type d'instance de performance à capacité extensible, et si vous prévoyez d'utiliser vos instances Spot de performance à capacité extensible immédiatement et pour une courte durée, sans temps d'inactivité pour accumuler des crédits processeur, nous vous recommandons de les lancer en [mode standard](#) pour éviter de payer des coûts plus élevés. Si vous lancez vos instances Spot de performance à capacité extensible en [mode Illimité](#) et que vous étendez immédiatement l'utilisation de l'UC, vous dépensez des crédits excédentaires pour cette extension d'utilisation. Si vous utilisez l'instance pour une courte durée, elle n'a pas le temps d'accumuler des crédits UC pour rembourser les crédits excédentaires, et ces derniers vous sont facturés lorsque vous résiliez l'instance.

Le mode Illimité convient aux instances Spot de performance à capacité extensible uniquement si l'instance s'exécute suffisamment longtemps pour accumuler des crédits UC pour l'extension d'utilisation. Sinon, payer des crédits excédentaires rend les instances Spot de performance à capacité extensible plus coûteuses que les autres instances. Pour plus d'informations, consultez [Quand utiliser le mode illimité/mode d'UC fixe ?](#).

Les instances T2, lorsqu'elles sont configurées en [mode Standard](#), obtiennent des [crédits de lancement](#). Les instances T2 sont les seules instances à capacité extensible qui obtiennent des crédits de lancement. Les crédits de lancement visent à optimiser la productivité du lancement initial des instances T2 en leur fournissant suffisamment de ressources de calcul pour pouvoir configurer l'instance. Il est interdit de procéder à des lancements répétés d'instances T2 pour bénéficier de nouveaux crédits de lancement. Si vous avez besoin de performances soutenues de l'UC, vous pouvez obtenir des crédits (en restant inactif pendant un certain temps) : utilisez le [mode Illimité](#) pour les Instances Spot T2 ou un type d'instance avec UC dédiée.

Hôtes dédiés

Un hôte dédié Amazon EC2 est un serveur physique entièrement dédié à votre usage. Vous pouvez éventuellement choisir de partager la capacité de l'instance avec d'autres AWS comptes. Pour plus d'informations, consultez [Utiliser des Hôtes dédiés partagés](#).

Les hôtes dédiés offrent une visibilité et un contrôle sur le placement des instances et favorisent l'affinité entre les hôtes. Cela signifie que vous pouvez lancer et exécuter des instances sur des hôtes spécifiques, et vous pouvez vous assurer que les instances ne s'exécutent que sur des hôtes spécifiques. Pour plus d'informations, consultez [Comprendre le placement automatique et l'affinité](#).

Les hébergeurs dédiés fournissent un support complet de licence BYOL (Bring Your Own License). Ils vous permettent d'utiliser vos licences logicielles existantes par socket, par cœur ou par machine virtuelle, notamment Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, ou d'autres licences logicielles liées à des machines virtuelles, des sockets ou des cœurs physiques, conformément aux termes de votre licence.

Si vous souhaitez que vos instances s'exécutent sur du matériel dédié, mais que vous n'avez pas besoin de visibilité ou de contrôle sur le placement des instances, et que vous n'avez pas besoin d'utiliser des licences logicielles par socket ou par cœur, vous pouvez envisager d'utiliser des instances dédiées à la place. Les instances dédiées et les hôtes dédiés peuvent tous deux être utilisés pour lancer des instances Amazon EC2 sur des serveurs physiques dédiés. Il n'existe pas de différence physique, de sécurité ou de performance entre les instances dédiées et les instances des Hôtes dédiés. Cependant, il existe des différences majeures entre eux. Le tableau suivant met en valeur quelques-unes des principales différences entre les Hôtes dédiés et les instances dédiées :

	Dedicated Host	Dedicated Instance
Serveur physique dédié	Serveur physique avec une capacité d'instance entièrement dédiée à votre utilisation.	Serveur physique dédié à un seul compte client.
Partage de capacité d'instance	Peut partager la capacité de l'instance avec d'autres comptes.	Non pris en charge
Facturation	Facturation par hôte	Facturation par instance

	Dedicated Host	Dedicated Instance
Visibilité des sockets, cœurs et ID d'hôte	Offre une visibilité sur le nombre de sockets et de cœurs physiques	Aucune visibilité
Affinité de l'hôte et de l'instance	Permet de déployer vos instances de façon cohérente sur le même serveur physique au fil du temps	Non pris en charge
Placement ciblé d'instances	Offre une visibilité supplémentaire et un contrôle sur la façon dont les instances sont placées sur un serveur physique	Non pris en charge
Récupération automatique des instances	Pris en charge. Pour plus d'informations, consultez Restauration de l'hôte .	Pris en charge
Bring Your Own License (Licence à fournir)	Pris en charge	Support partiel*
Réserve de capacité	Non pris en charge	Pris en charge

Serveur * Microsoft SQL avec License Mobility via Software Assurance et les licences Windows Virtual Desktop Access (VDA) peuvent être utilisées avec une instance dédiée.

Pour plus d'informations sur les instances dédiées, veuillez consulter la rubrique [Dedicated instances](#).

Table des matières

- [Configurations de capacité d'instance](#)
- [Bring Your Own License \(BYOL, licence à fournir\)](#)
- [Tarification et facturation](#)

- [instances T3 modulables sur les hôtes dédiés](#)
- [Restrictions Hôtes dédiés](#)
- [Utiliser Hôtes dédiés](#)
- [Utiliser des Hôtes dédiés partagées](#)
- [Hôtes dédiés sur AWS Outposts](#)
- [Restauration de l'hôte](#)
- [Maintenance de l'hôte](#)
- [Suivre les modifications de configuration](#)

Configurations de capacité d'instance

Les hôtes dédiés prennent en charge différentes configurations (cœurs physiques, sockets et processeurs virtuels) qui vous permettent d'exécuter des instances de familles et de tailles différentes.

Lorsque vous attribuez un hôte dédié à votre compte, vous pouvez choisir une configuration qui prend en charge soit un type d'instance unique ou plusieurs types d'instances au sein de la même famille d'instances. Le nombre d'instances que vous pouvez exécuter sur un hôte dépend de la configuration que vous choisissez.

Table des matières

- [Prise en charge d'un seul type d'instance](#)
- [Prise en charge de plusieurs types d'instances](#)

Prise en charge d'un seul type d'instance

Vous pouvez allouer un hôte dédié qui ne prend en charge qu'un seul type d'instance. Avec cette configuration, chaque instance que vous lancez sur l'hôte dédié doit être du même type d'instance, que vous spécifiez lors de l'allocation de l'hôte.

Par exemple, vous pouvez allouer un hôte qui prend uniquement en charge le type d'instance `m5.4xlarge`. Dans ce cas, vous pouvez exécuter uniquement des instances `m5.4xlarge` sur cet hôte.

Le nombre d'instances que vous pouvez lancer sur l'hôte dépend du nombre de cœurs physiques fournis par l'hôte et du nombre de cœurs utilisés par le type d'instance spécifié. Par exemple, si

vous attribuez un hôte à des instances `m5.4xlarge`, l'hôte fournit 48 cœurs physiques, et chaque instance `m5.4xlarge` consomme 8 cœurs physiques. Cela signifie que vous pouvez lancer jusqu'à 6 instances sur cet hôte (48 cœurs physiques/8 cœurs par instance = 6 instances).

Prise en charge de plusieurs types d'instances

Vous pouvez allouer un hôte dédié qui prend en charge plusieurs types d'instances au sein de la même famille d'instances. Cela vous permet d'exécuter différents types d'instances sur le même hôte, à condition qu'ils appartiennent à la même famille d'instances et que l'hôte dispose d'une capacité d'instance suffisante.

Par exemple, vous pouvez allouer un hôte qui prend en charge différents types d'instances au sein de la famille d'instances R5. Dans ce cas, vous pouvez lancer n'importe quelle combinaison de types d'instances R5, tels que `r5.large`, `r5.xlarge`, `r5.2xlarge` et `r5.4xlarge`, sur cet hôte, jusqu'à la capacité de cœur physique de l'hôte.

Les familles d'instances suivantes prennent en charge les hôtes dédiés et plusieurs types d'instances :

- Usage général : A1, M5, M5n, M6i et T3
- Optimisées pour le calcul : C5, C5n et C6i
- Mémoire optimisée : R5, R5n et R6i

Le nombre d'instances que vous pouvez exécuter sur l'hôte dépend du nombre de cœurs physiques fournis par l'hôte et du nombre de cœurs utilisés par chaque type d'instance exécuté sur l'hôte. Par exemple, si vous allouez un hôte R5, qui fournit 48 cœurs physiques, et que vous exécutez 2 instances `r5.2xlarge` (4 cœurs x 2 instances) et 3 instances `r5.4xlarge` (8 cœurs x 3 instances), ces instances utilisent au total 32 cœurs et vous pouvez exécuter n'importe quelle combinaison d'instances R5 tant qu'elles ne dépassent pas les 16 cœurs restants.

Cependant, pour chaque famille de l'instance, le nombre d'instances pouvant être exécutées pour chaque taille d'instance est limité. Par exemple, un hôte dédié R5 prend en charge jusqu'à 2 instances `r5.8xlarge`, ce qui utilise 32 des cœurs physiques. Dans ce cas, des instances R5 supplémentaires de tailles inférieures peuvent ensuite être utilisées pour remplir la capacité de l'hôte à la capacité cœur. Pour connaître le nombre de tailles d'instance prises en charge pour chaque famille d'instance, veuillez consulter la rubrique [Tableau de configuration des hôtes dédiés](#).

Le tableau suivant présente des exemples de combinaison de types d'instances :

Famille d'instances	Exemples de combinaisons de tailles d'instances	
R5	<ul style="list-style-type: none"> Exemple 1 : 4 x r5.4xlarge + 4 x r5.2xlarge Exemple 2 : 1 x r5.12xlarge + 1 x r5.4xlarge + 1 x r5.2xlarge + 5 x r5.xlarge + 2 x r5.large 	
C5	<ul style="list-style-type: none"> Exemple 1 : 1 x c5.9xlarge + 2 x c5.4xlarge + 1 x c5.xlarge Exemple 2 : 4 x c5.4xlarge + 1 x c5.xlarge + 2 x c5.large 	
M5	<ul style="list-style-type: none"> Exemple 1 : 4 x m5.4xlarge + 4 x m5.2xlarge Exemple 2 : 1 x m5.12xlarge + 1 x m5.4xlarge + 1 x m5.2xlarge + 5 x m5.xlarge + 2 x m5.large 	

Considérations

Gardez les points suivants à l'esprit lorsque vous travaillez avec des hôtes dédiés qui prennent en charge plusieurs types d'instances :

- Avec les hôtes dédiés de type N, tels que C5n, M5n et R5n, vous ne pouvez pas mélanger des tailles d'instance inférieures (2xlarge et inférieures) avec des tailles d'instance supérieures (4xlarge et supérieures, y compris metal). Si vous avez besoin d'utiliser simultanément des tailles d'instance inférieures et supérieures sur des hôtes dédiés de type N, vous devez allouer des hôtes distincts pour les tailles d'instance inférieures et supérieures.
- Nous vous recommandons de lancer d'abord les types d'instance supérieurs, puis de remplir la capacité d'instance restante avec les types d'instance inférieurs, si nécessaire.

Bring Your Own License (BYOL, licence à fournir)

Les Hôtes dédiés vous permettent d'utiliser vos licences logicielles existantes par socket, par cœur ou par machine virtuelle. Lorsque vous utilisez vos propres licences, vous êtes responsable de leur gestion. Toutefois, Amazon EC2 comporte des fonctionnalités qui vous aident à assurer la conformité de vos licences, telles que l'affinité d'instance et le placement ciblé.

Voici les grandes étapes que vous devez suivre afin d'utiliser votre propre image de machine virtuelle sous licence en volume dans Amazon EC2.

1. Assurez-vous que les termes du contrat de licence régissant l'utilisation de vos images de machine permettent l'utilisation dans un environnement cloud virtualisé. Pour de plus amples informations sur les licences Microsoft, consultez [Amazon Web Services et licences Microsoft](#).
2. Après avoir vérifié que votre image de machine peut être utilisée dans Amazon EC2, importez-la avec VM Import/Export. Pour plus d'informations sur la procédure à suivre pour importer votre image de machine, consultez le [Guide de l'utilisateur VM Import/Export](#).
3. Une fois votre image de machine importée, vous pouvez lancer des instances depuis cette image sur des Hôtes dédiés actifs de votre compte.
4. Lorsque vous exécutez ces instances, en fonction du système d'exploitation, vous pouvez être contraint d'activer ces instances sur votre propre serveur KMS (par exemple Windows Server ou Windows SQL Server). Vous ne pouvez pas activer votre AMI Windows importée sur le serveur KMS Windows Amazon.

Note

Pour suivre la façon dont vos images sont utilisées AWS, activez l'enregistrement par l'hôte dans AWS Config. Vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à un hôte dédié et utiliser la sortie comme source de données pour les rapports sur les licences. Pour plus d'informations, consultez [Suivre les modifications de configuration](#).

Tarification et facturation

Le prix d'un Hôte dédié varie selon l'option de paiement.

Options de paiement

- [Hôtes dédiés à la demande](#)
- [Dedicated Host Reservations](#)
- [Savings Plans](#)
- [Tarification pour Windows Server sur les Hôtes dédiés](#)

Hôtes dédiés à la demande

La facturation à la demande est automatiquement activée lorsque vous allouez un Hôte dédié à votre compte.

Le prix à la demande pour un Hôte dédié varie par famille de l'instance et par région. Vous payez par seconde (avec un minimum de 60 secondes) pour l'Hôte dédié actif, quelle que soit la quantité ou la taille des instances que vous choisissez de lancer dessus. Pour plus d'informations sur la tarification à la demande, consultez [Tarification à la demande des Amazon EC2 Hôtes dédiés](#).

Vous pouvez libérer un Hôte dédié à la demande à tout moment pour arrêter d'accumuler des frais dessus. Pour plus d'informations sur la libération d'un Hôte dédié, consultez [Créer des versions d'Hôtes dédiés](#).

Dedicated Host Reservations

Les réservations d'hôtes dédiés permettent de bénéficier d'une remise sur la facturation par rapport à l'exécution d'Hôtes dédiés à la demande. Trois options de paiement sont disponibles pour les réservations :

- **Aucun paiement initial** — Les réservations sans aucun paiement initial vous offrent une remise sur votre utilisation d'un Hôte dédié pendant une période donnée et ne nécessitent aucun paiement initial. Disponible pour une période d'un an ou de trois ans. Seules certaines familles d'instance prennent en charge le délai de trois ans pour les réservations sans aucun paiement initial.
- **Paiement initial partiel** — Une partie de la réservation doit être payée au départ et les heures restantes pendant la période sont facturées à un tarif réduit. Disponible pour une période d'un an ou de trois ans.
- **Paiement initial complet** — Offre le coût effectif le plus bas. Disponible pour une période d'un an et de trois ans et couvre le coût intégral de la période à l'avance, sans plus aucuns frais supplémentaire futurs.

Vous devez disposer d'un Hôte dédié actif sur votre compte pour pouvoir acheter des réservations. Chaque réservation peut couvrir un ou plusieurs hôtes prenant en charge la même famille de l'instance dans une seule zone de disponibilité. Les réservations sont appliquées à la famille de l'instance sur l'hôte, et non à la taille de l'instance. Si vous avez trois Hôtes dédiés avec des tailles d'instance différentes (`m4.xlarge`, `m4.medium` et `m4.large`), vous pouvez associer une même réservation `m4` à tous ces Hôtes dédiés. La famille de l'instance et la zone de disponibilité doivent correspondre à celles des hôtes dédiés que vous souhaitez leur associer.

Lorsqu'une réservation est associée à un Hôte dédié, cet Hôte dédié ne peut pas être libéré avant la fin de la période de la réservation.

Pour plus d'informations sur la tarification de réservation, consultez [Tarification d'un Hôte dédié Amazon EC2](#).

Savings Plans

Les Savings Plans sont un modèle de tarification flexible qui offre des économies importantes par rapport aux instances à la demande. Avec les Savings Plans, vous pouvez vous engager pour une utilisation continue, en USD par heure, pour une durée de un à trois ans. Cela vous donne la flexibilité d'utiliser le Hôte dédié répondant le mieux à vos besoins et de continuer à économiser de l'argent au lieu de vous engager pour un Hôte dédié spécifique. Pour plus d'informations, consultez le [Guide de l'utilisateur des AWS Savings Plans](#).

Note

Les Savings Plans (Plans d'épargne) ne sont pas pris en charge par `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, et `u-24tb1.metal` Hôtes dédiés.

Tarification pour Windows Server sur les Hôtes dédiés

Sous réserve des conditions de licence de Microsoft, vous pouvez importer vos licences Windows Server et SQL Server existantes vers les Hôtes dédiés. Aucuns frais supplémentaires ne s'applique à l'utilisation du logiciel si vous choisissez de réutiliser vos licences.

Vous pouvez également utiliser les AMI Windows Server fournies par Amazon pour exécuter les dernières versions de Windows Server sur des Hôtes dédiés. Il s'agit d'une pratique courante pour les scénarios où vous possédez des licences SQL Server existantes pouvant être exécutées sur des Hôtes dédiés, mais qui ont besoin de Windows Server pour exécuter la charge de travail SQL Server. Les AMI Windows Server fournies par Amazon ne sont prises en charge que sur les

types d'instances de la génération actuelle. Pour plus d'informations, consultez la [Tarification des hôtes dédiés Amazon EC2](#).

instances T3 modulables sur les hôtes dédiés

Les hôtes dédiés prennent en charge les instances T3 à performance modulable. Les instances T3 offrent un moyen économique d'utiliser votre logiciel de licence BYOL admissible sur du matériel dédié. L'encombrement vCPU réduit des instances T3 vous permet de consolider vos charges de travail sur moins d'hôtes et de maximiser l'utilisation de votre licence par cœur.

Les hôtes dédiés T3 sont les mieux adaptés pour exécuter le logiciel BYOL avec une utilisation faible à modérée du processeur. Cela inclut des licences logicielles éligibles par socket, par cœur ou par machine virtuelle, parmi lesquelles figurent Microsoft Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux et Oracle Database. Parmi les exemples des charges de travail adaptées aux Hôtes dédiés T3 se trouvent les petites et moyennes bases de données, les postes de travail virtuels, les environnements de développement et de test, les référentiels de code et les prototypes de produits. Les hôtes dédiés T3 ne sont pas recommandés pour les charges de travail avec une utilisation soutenue du processeur ou pour les charges de travail qui subissent simultanément des rafales de CPU corrélées.

Les instances T3 sur les hôtes dédiés utilisent le même modèle de crédit que les instances T3 sur le matériel de location partagé. Cependant, elles prennent uniquement en charge le mode de crédit standard ; le mode de crédit un*limited* n'est pas pris en charge. Dans le mode standard, les instances T3 sur les hôtes dédiés gagnent, dépensent et accumulent des crédits de la même manière que les instances extensibles sur le matériel de location partagé. Elles fournissent un niveau de base de performances du processeur, avec la possibilité de dépasser ce niveau en cas de besoin. Pour émettre en rafales au-dessus du niveau de base, l'instance dépense les crédits cumulés dans son solde de crédits UC. Lorsque les crédits accumulés sont épuisés, l'utilisation du processeur est réduite au niveau de référence. Pour plus d'informations sur le mode standard, consultez [Fonctionnement des instance de performance à capacité extensible standards](#).

Les hôtes dédiés T3 prennent en charge toutes les fonctionnalités offertes par les hôtes dédiés Amazon EC2, y compris les tailles d'instance multiples sur un seul hôte, les groupes de ressources d'hôte et BYOL.

Tailles et configurations d'instance T3 prises en charge

Les hôtes dédiés T3 exécutent des instances T3 à capacité extensible à usage général qui partagent les ressources CPU de l'hôte en fournissant une performance CPU de base et la possibilité

d'atteindre un niveau supérieur lorsque nécessaire. Cela permet aux hôtes dédiés T3, qui ont 48 cœurs, de prendre en charge un maximum de 192 instances par hôte. Afin d'utiliser efficacement les ressources de l'hôte et de fournir les meilleures performances d'instance, l'algorithme de placement d'instance Amazon EC2 calcule automatiquement le nombre d'instances prises en charge et les combinaisons de taille d'instance qui peuvent être lancées sur l'hôte.

Les hôtes dédiés T3 prennent en charge plusieurs types d'instance sur le même hôte. Les hôtes dédiés ne prennent pas en charge toutes les tailles d'instances T3. Vous pouvez exécuter différentes combinaisons d'instances T3 dans la limite du CPU de l'hôte.

Le tableau suivant répertorie les types d'instances pris en charge, résume les performances de chaque type d'instance et indique le nombre maximal d'instances pour chaque taille pouvant être lancées.

Type d'instance	vCPU	Mémoire (Gio)	Utilisation de référence du processeur par vCPU	Bande passante d'éclatement du réseau (Gbit/s)	Bande passante d'éclatement Amazon EBS (Mb/s)	Nombre maximal d'instances par hôte dédié
t3.nano	2	0.5	5 %	5	Jusqu'à 2 085	192
t3.micro	2	1	10 %	5	Jusqu'à 2 085	192
t3.small	2	2	20 %	5	Jusqu'à 2 085	192
t3.medium	2	4	20 %	5	Jusqu'à 2 085	192
t3.large	2	8	30 %	5	2 780	96
t3.xlarge	4	16	40 %	5	2 780	48
t3.2xlarge	8	32	40 %	5	2 780	24

Contrôler l'utilisation du processeur pour les hôtes dédiés T3

Vous pouvez utiliser la CloudWatch métrique `DedicatedHostCPUUtilization` Amazon pour surveiller l'utilisation des vCPU d'un hôte dédié. La métrique est disponible dans l'espace de noms

EC2 et dans la dimension `Per-Host-Metrics`. Pour plus d'informations, consultez [Métriques d'hôte dédié](#).

Restrictions Hôtes dédiés

Avant d'allouer des Hôtes dédiés, prenez note des restrictions suivantes :

- Pour exécuter RHEL, SUSE Linux et SQL Server sur Hôtes dédiés, vous devez apporter vos propres AMI. Les AMI RHEL, SUSE Linux et SQL Server proposées par AWS ou disponibles sur ne AWS Marketplace peuvent pas être utilisées avec des hôtes dédiés. Pour plus d'informations sur la création de votre propre AMI, consultez [Bring Your Own License \(BYOL, licence à fournir\)](#).

Cette restriction ne s'applique pas aux hôtes alloués aux instances de mémoire élevée (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` et `u-24tb1.metal`). Les AMI Linux RHEL et SUSE proposées par AWS ou disponibles sur ces hôtes AWS Marketplace peuvent être utilisées avec ces hôtes.

- Le nombre d'hôtes dédiés exécutés par famille d'instances, par compte AWS et par région est limité. Les quotas s'appliquent uniquement aux instances en cours d'exécution. Si votre instance est en attente, en cours d'arrêt ou arrêtée, elle n'est pas prise en compte dans votre quota. Pour consulter les quotas s'appliquant à votre compte, ou pour demander une augmentation de quota, utilisez la [console Service Quotas](#).
- Les instances qui fonctionnent sur un Hôte dédié ne peuvent être lancées que dans un VPC.
- Les groupes Auto Scaling sont pris en charge lors de l'utilisation d'un modèle de lancement qui spécifie un groupe de ressources hôte. Pour plus d'informations, consultez la section [Création d'un modèle de lancement à l'aide de paramètres avancés](#) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.
- Les instances Amazon RDS ne sont pas prises en charge.
- Le niveau d'utilisation AWS gratuite n'est pas disponible pour les hôtes dédiés.
- Le contrôle de placement d'instance fait référence à la gestion du lancement d'instances sur les Hôtes dédiés. Vous ne pouvez pas lancer Hôtes dédiés dans des groupes de placement.
- Si vous allouez un hôte pour un type d'instance virtualisée, vous ne pouvez pas modifier le type d'instance en un type d'instance `.metal` après l'allocation de l'hôte. Par exemple, si vous allouez un hôte pour le type d'instance `m5.large`, vous ne pouvez pas modifier le type d'instance en `m5.metal`.

De même, si vous allouez un hôte pour un type d'instance `.metal`, vous ne pouvez pas modifier le type d'instance en un type d'instance virtualisée après l'allocation de l'hôte. Par exemple, si vous

allouez un hôte pour le type d'instance `m5.metal`, vous ne pouvez pas modifier le type d'instance en `m5.large`.

Utiliser Hôtes dédiés

Pour utiliser un Hôte dédié, vous devez d'abord allouer des hôtes à utiliser sur votre compte. Vous pouvez ensuite lancer des instances sur les hôtes en spécifiant une location d'hôte pour l'instance. Vous devez sélectionner un hôte spécifique sur lequel lancer l'instance, ou vous pouvez autoriser son lancement sur n'importe quel hôte sur lequel le placement automatique est activé et qui correspond à son type d'instance. Lorsqu'une instance est arrêtée puis redémarrée, le paramètre d'affinité de l'hôte détermine si elle est redémarrée sur le même hôte ou sur un autre.

Si vous n'avez plus besoin d'un hôte à la demande, vous pouvez arrêter les instances en cours d'exécution sur celui-ci, configurer leur lancement sur un autre hôte, puis libérer l'hôte.

Les hôtes dédiés sont également intégrés à AWS License Manager. Grâce à License Manager, vous pouvez créer un groupe de ressources hôte, qui est un ensemble d'Hôtes dédiés gérés en tant qu'entité unique. Lors de la création d'un groupe de ressources hôte, vous spécifiez les préférences de gestion de l'hôte, telles que l'allocation automatique et la libération automatique, pour les Hôtes dédiés. Vous pouvez ainsi lancer des instances sur les Hôtes dédiés sans allouer ni gérer manuellement ces hôtes. Pour plus d'informations, consultez [Groupes de ressources hôte](#) dans le Guide de l'utilisateur AWS License Manager .

Sommaire

- [Allouer des Hôtes dédiés](#)
- [Lancer des instances sur un Hôte dédié](#)
- [Lancer des instances dans un groupe de ressources hôte](#)
- [Comprendre le placement automatique et l'affinité](#)
- [Modifier le placement automatique d'Hôte dédié](#)
- [Modifier les types d'instance pris en charge](#)
- [Modifier l'affinité et la location d'une instance](#)
- [Afficher les Hôtes dédiés](#)
- [Balisage des Hôtes dédiés](#)
- [Surveiller les Hôtes dédiés](#)
- [Créer des versions d'Hôtes dédiés](#)

- [Acheter des réservations d'hôtes dédiés](#)
- [Afficher les réservations d'Hôte dédié](#)
- [Baliser les réservations d'hôtes dédiés](#)

Allouer des Hôtes dédiés

Pour commencer à utiliser des Hôtes dédiés, vous devez allouer des Hôtes dédiés à votre compte à l'aide de la console Amazon EC2 ou des outils de ligne de commande. Lorsque vous allouez l'Hôte dédié, la capacité de l'Hôte dédié est immédiatement mise à disposition dans votre compte et vous pouvez commencer à lancer des instances sur l'Hôte dédié.

Lorsque vous attribuez un hôte dédié à votre compte, vous pouvez choisir une configuration qui prend en charge soit un type d'instance unique ou plusieurs types d'instances au sein de la même famille d'instances. Le nombre d'instances que vous pouvez exécuter sur l'hôte dépend de la configuration que vous choisissez. Pour plus d'informations, consultez [Configurations de capacité d'instance](#).

Console

Pour allouer un Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Hôtes dédiés, puis Allouer un Hôte dédié.
3. Pour Famille d'instances, choisissez la famille de l'instance de l'Hôte dédié.
4. Indiquez si l'Hôte dédié prend en charge plusieurs types d'instances dans la famille d'instances sélectionnée ou uniquement un type d'instance spécifique. Effectuez l'une des actions suivantes :
 - Pour configurer l'Hôte dédié afin qu'il prenne en charge plusieurs types d'instances dans la famille d'instances sélectionnée, pour Support multiple instance types (Prendre en charge plusieurs types d'instances), choisissez Activer. La sélection de cette option vous permet de lancer différentes tailles d'instances d'une même famille d'instances sur l'Hôte dédié. Par exemple, si vous choisissez la famille d'instances m5 et que vous choisissez cette option, vous pouvez lancer les instances m5.xlarge et m5.4xlarge sur l'Hôte dédié.
 - Pour configurer l'hôte dédié afin qu'il prenne en charge un type d'instance spécifique dans la famille d'instances sélectionnée, désélectionnez Support multiple instance types (Prendre en charge plusieurs types d'instances), puis, dans Instance type (Type

d'instance), choisissez le type d'instance à prendre en charge. Cette action vous permet de lancer un seul type d'instance sur l'Hôte dédié. Par exemple, si vous choisissez cette option et spécifiez `m5.4xlarge` comme type d'instance pris en charge, vous pouvez uniquement lancer des instances `m5.4xlarge` sur l'Hôte dédié.

5. Pour Zone de disponibilité, choisissez la zone de disponibilité dans laquelle allouer l'Hôte dédié.
6. Pour autoriser l'Hôte dédié à accepter les lancements d'instance non ciblés correspondant à son type d'instance, pour Instance auto-placement (Placement automatique d'instance), choisissez Enable (Autoriser). Pour en savoir plus sur le placement automatique, consultez [Comprendre le placement automatique et l'affinité](#).
7. Pour autoriser la récupération d'hôte pour l'Hôte dédié, pour Host recovery (Récupération de l'hôte), choisissez Activer. Pour plus d'informations, consultez [Restauration de l'hôte](#).
8. Pour Quantité, entrez le nombre d'Hôtes dédiés à allouer.
9. (Facultatif) Sélectionnez Ajouter une nouvelle balise et saisissez une clé et une valeur de balise.
10. Choisissez Allocate.

AWS CLI

Pour allouer un Hôte dédié

Utilisez la commande [allocate-hosts](#) AWS CLI . La commande suivante alloue un Hôte dédié qui prend en charge plusieurs types d'instances de la famille d'instances `m5` dans la zone de disponibilité `us-east-1a`. La fonction de récupération de l'hôte est activée et la fonction de placement automatique est désactivée sur l'hôte.

```
aws ec2 allocate-hosts --instance-family "m5" --availability-zone "us-east-1a" --auto-placement "off" --host-recovery "on" --quantity 1
```

La commande suivante alloue un Hôte dédié qui prend en charge des lancements d'instance `m4.large` non ciblés dans la zone de disponibilité `eu-west-1a`, autorise la récupération de l'hôte et applique une balise avec une clé `purpose` et une valeur `production`.

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a" --auto-placement "on" --host-recovery "on" --quantity 1 --tag-specifications 'ResourceType=dedicated-host,Tags=[{Key=purpose,Value=production}]'
```

PowerShell

Pour allouer un Hôte dédié

Utilisez la [New-EC2Host](#) AWS Tools for Windows PowerShell commande. La commande suivante alloue un Hôte dédié qui prend en charge plusieurs types d'instances de la famille d'instances m5 dans la zone de disponibilité us-east-1a. La fonction de récupération de l'hôte est activée et la fonction de placement automatique est désactivée sur l'hôte.

```
PS C:\> New-EC2Host -InstanceFamily m5 -AvailabilityZone us-east-1a -  
AutoPlacement Off -HostRecovery On -Quantity 1
```

Les commandes suivantes allouent un Hôte dédié qui prend en charge des lancements d'instance non ciblés m4.large dans la zone de disponibilité eu-west-1a et appliquent une balise avec une clé purpose et une valeur production.

Le paramètre TagSpecification utilisé pour baliser un Hôte dédié à la création requiert un objet qui spécifie le type de ressource à baliser, ainsi que la clé et la valeur de balise. Les commandes suivantes permettent de créer l'objet requis.

```
PS C:\> $tag = @{ Key="purpose"; Value="production" }  
PS C:\> $tagspec = new-object Amazon.EC2.Model.TagSpecification  
PS C:\> $tagspec.ResourceType = "dedicated-host"  
PS C:\> $tagspec.Tags.Add($tag)
```

La commande suivante alloue le Hôte dédié et applique la balise spécifiée dans l'objet \$tagspec.

```
PS C:\> New-EC2Host -InstanceType m4.large -AvailabilityZone eu-west-1a -  
AutoPlacement On -HostRecovery On -Quantity 1 -TagSpecification $tagspec
```

Lancer des instances sur un Hôte dédié

Une fois que vous avez alloué un Hôte dédié, vous pouvez lancer des instances sur cet hôte. Vous ne pouvez pas lancer des instances avec la location host si vous n'avez pas d'Hôtes dédiés actifs avec suffisamment de capacité disponible pour le type d'instance que vous lancez.

i Tip

Pour les hôtes dédiés qui prennent en charge plusieurs tailles d'instance, nous vous recommandons de lancer d'abord les instances de plus grande taille, puis de remplir la capacité d'instance restante avec les instances de plus petite taille, si nécessaire.

Avant de lancer vos instances, prenez note des restrictions. Pour plus d'informations, consultez [Restrictions Hôtes dédiés](#).

Vous pouvez lancer une instance dans un Hôte dédié à l'aide des méthodes suivantes.

Console

Pour lancer une instance sur un Hôte dédié spécifique depuis la page Hôtes dédiés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Hôtes dédiés dans le volet de navigation.
3. Dans la page Dedicated Hosts (Hôtes dédiés), sélectionnez un hôte et choisissez Actions, Launch Instance(s) onto host (Lancer une ou plusieurs instances sur l'hôte).
4. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez une AMI de la liste.

i Note

Les AMI SQL Server, SUSE et RHEL fournies par Amazon EC2 ne peuvent pas être utilisées avec des Hôtes dédiés.

5. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance à lancer.

i Note

Si l'Hôte dédié ne prend en charge qu'un seul type d'instance, ce type est sélectionné par défaut et ne peut pas être modifié.

Si l'Hôte dédié prend en charge plusieurs types d'instances, vous devez sélectionner un type d'instance dans la famille d'instances prise en charge en fonction de la capacité d'instance disponible de l'Hôte dédié. Nous vous recommandons de lancer

d'abord les tailles d'instance plus grandes, puis de remplir la capacité d'instance restante avec les tailles d'instance plus petites, si nécessaire.

6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à associer à l'instance.
7. Dans la section Advanced details (Détails avancés), pour Tenancy affinity (Affinité de location), sélectionnez l'une des options suivantes :
 - Sélectionnez Off (Désactivé) — L'instance est lancée sur l'hôte spécifié, mais il n'est pas garanti qu'elle redémarre sur le même hôte dédié si elle est arrêtée.
 - Sélectionnez l'ID de l'hôte dédié — Si l'instance est arrêtée, elle redémarre toujours sur cet hôte spécifique.

Pour en savoir plus sur l'affinité, consultez [Comprendre le placement automatique et l'affinité](#).

 Note

Les options Location et Hôte sont préconfigurées en fonction de l'hôte que vous avez sélectionné.

8. Configurez les options d'instance restantes selon les besoins. Pour plus d'informations, consultez [Lancer une instance à l'aide de paramètres définis](#).
9. Sélectionnez Launch instance (Lancer une instance).

Pour lancer une instance sur un Hôte dédié à l'aide de l'assistant de lancement d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances, Launch instance (Lancer une instance).
3. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez une AMI de la liste.

 Note

Les AMI SQL Server, SUSE et RHEL fournies par Amazon EC2 ne peuvent pas être utilisées avec des Hôtes dédiés.

4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance à lancer.
5. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à associer à l'instance.
6. Dans la section Advanced details (Détails avancés), procédez comme suit :
 - a. Pour Tenancy (Location), sélectionnez Dedicated Host (Hôte dédié).
 - b. Pour Target host by (Cibler l'hôte par), sélectionnez Host ID (ID de l'hôte).
 - c. Pour Target host ID (ID de l'hôte cible), sélectionnez l'hôte sur lequel lancer l'instance.
 - d. Pour Tenancy affinity (Affinité de location), sélectionnez l'une des options suivantes :
 - Sélectionnez Off (Désactivé) — L'instance est lancée sur l'hôte spécifié, mais il n'est pas garanti qu'elle redémarre sur le même hôte dédié si elle est arrêtée.
 - Sélectionnez l'ID de l'hôte dédié — Si l'instance est arrêtée, elle redémarre toujours sur cet hôte spécifique.

Pour en savoir plus sur l'affinité, consultez [Comprendre le placement automatique et l'affinité](#).

7. Configurez les options d'instance restantes selon les besoins. Pour plus d'informations, consultez [Lancer une instance à l'aide de paramètres définis](#).
8. Sélectionnez Launch instance (Lancer une instance).

AWS CLI

Pour lancer une instance dans un Hôte dédié

Utilisez la AWS CLI commande [run-instances](#) et spécifiez l'affinité, la location et l'hôte de l'instance dans le Placement paramètre de requête.

PowerShell

Pour lancer une instance dans un Hôte dédié

Utilisez la [New-EC2Instance](#) AWS Tools for Windows PowerShell commande et spécifiez l'affinité, la location et l'hôte de l'instance dans le paramètre de Placement demande.

Lancer des instances dans un groupe de ressources hôte

Lorsque vous lancez une instance dans un groupe de ressources hôte qui contient un Hôte dédié avec une capacité d'instance disponible, Amazon EC2 lance l'instance sur cet hôte. Si le groupe de

ressources hôte ne contient pas d'hôte avec une capacité d'instance disponible, Amazon EC2 alloue automatiquement un nouvel hôte dans le groupe de ressources hôte, puis lance l'instance sur cet hôte. Pour plus d'informations, consultez [Groupes de ressources hôte](#) dans le Guide de l'utilisateur AWS License Manager .

Exigences et limites

- Vous devez associer une configuration de licence basée sur le cœur/socket à l'AMI.
- Vous ne pouvez pas utiliser les AMI SQL Server, SUSE ou RHEL fournies par Amazon EC2 avec Hôtes dédiés.
- Vous ne pouvez pas cibler un hôte spécifique en choisissant un ID d'hôte et vous ne pouvez pas activer l'affinité d'instance lors du lancement d'une instance dans un groupe de ressources hôte.

Vous pouvez lancer une instance dans un groupe de ressources hôte à l'aide des méthodes suivantes.

Console

Pour lancer une instance dans un groupe de ressources hôte

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances, Launch instance (Lancer une instance).
3. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez une AMI de la liste.

Note

Les AMI SQL Server, SUSE et RHEL fournies par Amazon EC2 ne peuvent pas être utilisées avec des Hôtes dédiés.

4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance à lancer.
5. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à associer à l'instance.
6. Dans la section Advanced details (Détails avancés), procédez comme suit :
 - a. Pour Tenancy (Location), sélectionnez Dedicated Host (Hôte dédié).

- b. Pour Target host by (Cibler l'hôte par), sélectionnez Host resource group (Groupe de ressources hôte).
- c. Pour Host resource group name (Groupe de ressources hôte de location), sélectionnez le groupe de ressources hôte dans lequel lancer l'instance.
- d. Pour Tenancy affinity (Affinité de location), sélectionnez l'une des options suivantes :
 - Sélectionnez Off (Désactivé) — L'instance est lancée sur l'hôte spécifié, mais il n'est pas garanti qu'elle redémarre sur le même hôte dédié si elle est arrêtée.
 - Sélectionnez l'ID de l'hôte dédié — Si l'instance est arrêtée, elle redémarre toujours sur cet hôte spécifique.

Pour en savoir plus sur l'affinité, consultez [Comprendre le placement automatique et l'affinité](#).

7. Configurez les options d'instance restantes selon les besoins. Pour plus d'informations, consultez [Lancer une instance à l'aide de paramètres définis](#).
8. Sélectionnez Launch instance (Lancer une instance).

AWS CLI

Pour lancer une instance dans un groupe de ressources hôte

Utilisez la AWS CLI commande [run-instances](#) et, dans le paramètre de Placement requête, omettez l'option Tenancy et spécifiez l'ARN du groupe de ressources hôte.

PowerShell

Pour lancer une instance dans un groupe de ressources hôte

Utilisez la [New-EC2Instance](#) AWS Tools for Windows PowerShell commande et, dans le paramètre de Placement requête, omettez l'option Tenancy et spécifiez l'ARN du groupe de ressources hôtes.

Comprendre le placement automatique et l'affinité

Le contrôle de placement pour l'Hôtes dédiés est effectué au niveau de l'instance et au niveau de l'hôte.

Placement automatique

Le placement automatique est configuré au niveau de l'hôte. Il vous permet de définir si les instances que vous lancez le sont sur un hôte spécifique ou sur n'importe quel hôte disponible doté de configurations correspondantes.

Lorsque le placement automatique d'un Hôte dédié est désactivé, il n'accepte que les lancements d'instance de location d'hôte qui spécifient son ID d'hôte unique. Il s'agit du paramètre par défaut pour un nouvel Hôtes dédiés.

Lorsque le placement automatique d'un Hôte dédié est activé, il accepte tous les lancements d'instances non ciblés qui correspondent à la configuration de son type d'instance.

Lors du lancement d'une instance, vous devez configurer sa location. Le lancement d'une instance sur un Hôte dédié sans indiquer un `HostId` spécifique permet de la lancer sur n'importe quel Hôte dédié sur lequel le placement automatique est activé et qui correspond à son type d'instance.

Affinité de l'hôte

L'affinité de l'hôte est configurée au niveau de l'instance. Elle établit une relation de lancement entre une instance et un Hôte dédié.

Lorsque l'affinité a pour valeur `Host`, une instance lancée sur un hôte spécifique redémarre toujours sur le même hôte si elle est arrêtée. Cela s'applique aussi bien aux lancements ciblés qu'aux lancements non-ciblés.

Lorsque l'affinité a pour valeur `Default` et que vous arrêtez et redémarrez l'instance, cette dernière peut être redémarrée sur tout hôte disponible. Toutefois, elle essaie de se relancer sur le dernier Hôte dédié sur lequel elle s'est exécutée (dans la mesure du possible).

Modifier le placement automatique d'Hôte dédié

Vous pouvez modifier les paramètres de placement automatique d'un hôte dédié après l'avoir attribué à votre AWS compte, en utilisant l'une des méthodes suivantes.

Console

Pour modifier le placement automatique d'un Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez un hôte et choisissez Actions, Modify host (Modifier l'hôte).
4. Pour Instance auto-placement (Placement automatique de l'instance), choisissez Activer pour activer le placement automatique ou Désactiver pour désactiver le placement automatique. Pour plus d'informations, consultez [Comprendre le placement automatique et l'affinité](#).
5. Choisissez Enregistrer.

AWS CLI

Pour modifier le placement automatique d'un Hôte dédié

Utilisez la commande [modify-hosts](#) AWS CLI . Les exemples suivants activent le placement automatique pour l'Hôte dédié spécifié.

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

PowerShell

Pour modifier le placement automatique d'un Hôte dédié

Utilisez la [Edit-EC2Host](#) AWS Tools for Windows PowerShell commande. Les exemples suivants activent le placement automatique pour l'Hôte dédié spécifié.

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

Modifier les types d'instance pris en charge

La prise en charge de plusieurs types d'instance sur le même hôte dédié est disponible pour les familles d'instances suivantes : C5, M5, R5, C5n, R5n, M5n et T3. Les autres familles d'instances ne prennent en charge qu'un seul type d'instance sur le même Hôte dédié.

Vous pouvez allouer un Hôte dédié à l'aide des méthodes suivantes.

Vous pouvez modifier un Hôte dédié afin de modifier les types d'instances qu'il prend en charge. S'il prend actuellement en charge un seul type d'instance, vous pouvez le modifier afin qu'il en prenne en charge plusieurs dans cette famille d'instances. De même, s'il prend en charge plusieurs types d'instances, vous pouvez le modifier afin qu'il n'en prenne plus qu'un seul.

Pour modifier un Hôte dédié afin qu'il prenne en charge plusieurs types d'instances, vous devez d'abord arrêter toutes les instances en cours d'exécution sur l'hôte. Cette modification prend effet au bout d'environ 10 minutes. L'Hôte dédié passe à l'état `pending` pendant que la modification est en cours. Vous ne pouvez pas démarrer les instances arrêtées ou lancer de nouvelles instances sur l'Hôte dédié lorsqu'il est à l'état `pending`.

Pour qu'il soit possible de modifier un Hôte dédié prenant en charge plusieurs types d'instances afin qu'il n'en prenne plus qu'un seul, l'hôte ne doit avoir aucune instance en cours d'exécution ou les instances en cours d'exécution doivent être du type qui devra être pris en charge par l'hôte. Par exemple, pour modifier un hôte prenant en charge plusieurs types d'instances dans la famille d'instances `m5` afin qu'il ne prenne plus en charge que les instances `m5.large`, il faut que l'Hôte dédié n'ait aucune instance en cours d'exécution ou que seules des instances `m5.large` soient en cours d'exécution sur l'hôte.

Si vous allouez un hôte pour un type d'instance virtualisée, vous ne pouvez pas modifier le type d'instance en un type d'instance `.metal` après l'allocation de l'hôte. Par exemple, si vous allouez un hôte pour le type d'instance `m5.large`, vous ne pouvez pas modifier le type d'instance en `m5.metal`. De même, si vous allouez un hôte pour un type d'instance `.metal`, vous ne pouvez pas modifier le type d'instance en un type d'instance virtualisée après l'allocation de l'hôte. Par exemple, si vous allouez un hôte pour le type d'instance `m5.metal`, vous ne pouvez pas modifier le type d'instance en `m5.large`.

Vous pouvez modifier les types d'instance pris en charge à l'aide de l'une des méthodes suivantes.

Console

Pour modifier les types d'instance pris en charge pour un Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez `Dedicated Host` (Hôte dédié).
3. Sélectionnez l'Hôte dédié à modifier et choisissez `Actions, Modify host` (Modifier l'hôte).
4. Selon la configuration actuelle de l'Hôte dédié, procédez comme indiqué ci-après.
 - Si l'Hôte dédié prend actuellement en charge un type d'instance spécifique, l'option `Support multiple instance types` (Prendre en charge plusieurs types d'instance) n'est pas activée et la liste `Type d'instance` répertorie le type d'instance pris en charge. Pour modifier l'hôte afin qu'il prenne en charge plusieurs types d'instances dans la famille d'instances actuelle, pour `Support multiple instance types` (Prendre en charge plusieurs types d'instances), choisissez `Activer`.

Pour modifier un hôte afin qu'il prenne en charge plusieurs types d'instances, vous devez d'abord arrêter toutes les instances en cours d'exécution sur l'hôte.

- Si l'Hôte dédié prend actuellement en charge plusieurs types d'instances d'une famille, **Activé** est sélectionné pour **Support multiple instance types** (Prendre en charge plusieurs types d'instances). Pour modifier l'hôte afin qu'il prenne en charge un type d'instance spécifique, pour **Support multiple instance types** (Prendre en charge plusieurs types d'instances), décochez **Activer**, puis pour **Type d'instance**, sélectionnez le type d'instance spécifique à prendre en charge.

Vous ne pouvez pas modifier la famille d'instances prise en charge par l'Hôte dédié.

5. Choisissez **Enregistrer**.

AWS CLI

Pour modifier les types d'instance pris en charge pour un Hôte dédié

Utilisez la commande [modify-hosts](#) AWS CLI .

La commande suivante modifie un Hôte dédié afin qu'il prenne en charge plusieurs types d'instances au sein de la famille d'instances m5.

```
aws ec2 modify-hosts --instance-family m5 --host-ids h-012a3456b7890cdef
```

La commande suivante modifie un Hôte dédié afin qu'il prenne uniquement en charge les instances m5.xlarge.

```
aws ec2 modify-hosts --instance-type m5.xlarge --instance-family --host-ids h-012a3456b7890cdef
```

PowerShell

Pour modifier les types d'instance pris en charge pour un Hôte dédié

Utilisez la [Edit-EC2Host](#) AWS Tools for Windows PowerShell commande.

La commande suivante modifie un Hôte dédié afin qu'il prenne en charge plusieurs types d'instances au sein de la famille d'instances m5.

```
PS C:\> Edit-EC2Host --InstanceFamily m5 --HostId h-012a3456b7890cdef
```

La commande suivante modifie un Hôte dédié afin qu'il prenne uniquement en charge les instances `m5.xlarge`.

```
PS C:\> Edit-EC2Host --InstanceType m5.xlarge --HostId h-012a3456b7890cdef
```

Modifier l'affinité et la location d'une instance

Vous pouvez modifier la location d'une instance après l'avoir lancée. Vous pouvez également modifier l'affinité de votre instance afin de cibler un hôte spécifique ou de l'autoriser à être lancée sur n'importe quel hôte dédié disponible avec les attributs correspondants dans votre compte. Pour qu'il soit possible de modifier l'affinité ou la location de l'instance, il faut que l'instance soit à l'état `stopped`.

Les détails du système d'exploitation de votre instance, et le fait que SQL Server soit installé ou non, ont une incidence sur les conversions prises en charge. Pour plus d'informations sur les chemins de conversion de location disponibles pour votre instance, consultez la section [Tenancy conversion](#) dans le Guide de l'utilisateur de License Manager.

Note

Pour les instances T3, vous devez lancer l'instance sur un hôte dédié pour utiliser une location `host`. Pour les instances T3, vous ne pouvez pas modifier la location de `host` à `dedicated` ou `default`. Si vous tentez d'effectuer l'une de ces modifications de location non prises en charge, vous obtiendrez un code d'erreur `InvalidRequest`.

Vous pouvez modifier la location et l'affinité d'une instance à l'aide des méthodes suivantes.

Console

Pour modifier la location d'instance ou l'affinité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Instances, puis sélectionnez l'instance à modifier.
3. Choisissez État de l'instance, Arrêter.

4. Tandis que l'instance est toujours sélectionnée, choisissez Actions, Paramètres de l'instance, puis Changer le placement d'instance.
5. Sur la page Modifier le placement de l'instance, configurez les éléments suivants :
 - Location — Choisissez l'une des options suivantes :
 - Exécuter une instance matérielle dédiée — Lance l'instance en tant qu'Instance dédiée. Pour plus d'informations, consultez [Dedicated instances](#).
 - Launch the instance on a Hôte dédié — Lance l'instance sur un Hôte dédié avec une affinité configurable.
 - Affinité — Choisissez l'une des options suivantes :
 - Cette instance peut être exécutée sur un de mes hôtes — L'instance est lancée sur n'importe quel Hôte dédié disponible de votre compte prenant en charge son type d'instance.
 - Cette instance ne peut être exécutée que sur l'hôte sélectionné — L'instance ne peut s'exécuter que sur l'Hôte dédié sélectionné pour Hôte cible.
 - Hôte cible — Sélectionnez l'Hôte dédié sur lequel l'instance doit s'exécuter. Si aucun hôte cible n'est répertorié, cela signifie que vous n'avez peut-être aucun Hôtes dédiés compatible disponible dans votre compte.

Pour plus d'informations, consultez [Comprendre le placement automatique et l'affinité](#).

6. Choisissez Enregistrer.

AWS CLI

Pour modifier la location d'instance ou l'affinité

Utilisez la commande [AWS CLI modify-instance-placement](#). Les exemples suivants remplacent l'affinité de l'instance spécifiée default par host et indiquent l'Hôte dédié avec lequel l'instance a une affinité.

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host
--tenancy host --host-id h-012a3456b7890cdef
```

PowerShell

Pour modifier la location d'instance ou l'affinité

Utilisez la [Edit-EC2InstancePlacement](#) AWS Tools for Windows PowerShell commande. Les exemples suivants remplacent l'affinité de l'instance spécifiée default par host et indiquent l'Hôte dédié avec lequel l'instance a une affinité.

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -  
Tenancy host -HostId h-012a3456b7890cdef
```

Afficher les Hôtes dédiés

Vous pouvez afficher des détails sur un Hôte dédié et les instances individuelles qui s'y trouvent à l'aide des méthodes suivantes.

Console

Pour afficher les détails d'un Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sur la page Hôtes dédiés, sélectionnez un hôte.
4. Pour plus d'informations sur l'hôte, choisissez Détails.

Available vCPUs (UC virtuelles disponibles) indique les UC virtuelles (vCPU) qui sont disponibles sur l'Hôte dédié pour les nouveaux lancements d'instances. Par exemple, un Hôte dédié prenant en charge plusieurs types d'instances dans la famille d'instances c5 et ne possédant aucune instance en cours d'exécution possède 72 UC virtuelles disponibles. Cela signifie que vous pouvez lancer différentes combinaisons de types d'instances sur l'Hôte dédié pour consommer les 72 UC virtuelles disponibles.

Pour obtenir des informations sur les instances en cours d'exécution sur l'hôte, choisissez Instances en cours d'exécution.

AWS CLI

Pour afficher la capacité d'un Hôte dédié

Utilisez la commande [describe-hosts](#) AWS CLI .

L'exemple suivant utilise la commande [describe-hosts](#) (AWS CLI) pour afficher la capacité d'instance disponible d'un hôte dédié prenant en charge plusieurs types d'instances au sein de

la famille d'instances c5. L'Hôte dédié possède déjà deux instances c5.4xlarge et quatre instances c5.2xlarge en cours d'exécution.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

```
"AvailableInstanceCapacity": [  
  { "AvailableCapacity": 2,  
    "InstanceType": "c5.xlarge",  
    "TotalCapacity": 18 },  
  { "AvailableCapacity": 4,  
    "InstanceType": "c5.large",  
    "TotalCapacity": 36 }  
],  
"AvailableVCpus": 8
```

PowerShell

Pour afficher la capacité d'instance d'un Hôte dédié

Utilisez la [Get-EC2Host](#) AWS Tools for Windows PowerShell commande.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

Balisage des Hôtes dédiés

Vous pouvez allouer des balises personnalisées à vos entités Hôte dédié existantes pour classer celles-ci de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Cela vous aide à trouver rapidement un hôte dédié spécifique en fonction des balises personnalisées que vous lui avez attribuées. Les balises hôtes dédiées peuvent également être utilisées pour le suivi de la répartition des coûts.

Vous pouvez aussi appliquer des balises aux Hôtes dédiés lors de la création. Pour plus d'informations, consultez [Allouer des Hôtes dédiés](#).

Vous pouvez attribuer des balises à un Hôte dédié à l'aide des méthodes suivantes.

Console

Pour attribuer des balises à un Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'Hôte dédié auquel attribuer des balises, puis choisissez Actions, Gérer les balises.
4. Dans l'écran Gérer les balises, choisissez Ajouter la balise, puis spécifiez la clé et la valeur de la balise.
5. (Facultatif) Choisissez Ajouter la balise pour ajouter des balises supplémentaires à l'Hôte dédié.
6. Sélectionnez Save Changes.

AWS CLI

Pour attribuer des balises à un Hôte dédié

Utilisez la commande [create-tags](#) AWS CLI .

La commande suivante ajoute la balise `Owner=TeamA` à l'Hôte dédié spécifié.

```
aws ec2 create-tags --resources h-abc12345678909876 --tags Key=Owner,Value=TeamA
```

PowerShell

Pour attribuer des balises à un Hôte dédié

Utilisez la [New-EC2Tag](#) AWS Tools for Windows PowerShell commande.

La commande `New-EC2Tag` nécessite un objet `Tag`, qui spécifie la paire clé-valeur à utiliser pour la balise d'Hôte dédié. Les commandes suivantes créent un objet `Tag` nommé `$tag` avec une paire clé-valeur `Owner` et `TeamA` :

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag  
PS C:\> $tag.Key = "Owner"  
PS C:\> $tag.Value = "TeamA"
```

La commande suivante balise l'Hôte dédié spécifié avec l'objet `$tag` :

```
PS C:\> New-EC2Tag -Resource h-abc12345678909876 -Tag $tag
```

Surveiller les Hôtes dédiés

Amazon EC2 surveille constamment l'état de vos Hôtes dédiés. Les mises à jour sont communiquées sur la console Amazon EC2. Vous pouvez afficher des informations sur un Hôte dédié à l'aide des méthodes suivantes.

Console

Pour afficher l'état d'un Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Recherchez l'Hôte dédié dans la liste et consultez la valeur située dans la colonne État.

AWS CLI

Pour afficher l'état d'un Hôte dédié

Utilisez la AWS CLI commande [describe-hosts](#), puis examinez la state propriété dans l'élément de hostSet réponse.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

Pour afficher l'état d'un Hôte dédié

Utilisez la [Get-EC2Host](#) AWS Tools for Windows PowerShell commande, puis passez en revue la state propriété dans l'élément de hostSet réponse.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

Le tableau suivant explique les états possibles pour l'Hôte dédié.

État	Description
available	AWS n'a détecté aucun problème avec l'hôte dédié. Aucune maintenance ni réparation n'est programmée. Les instances peuvent être lancées sur cet hôte dédié.

État	Description
released	L'Hôte dédié a été libéré. l'ID de l'hôte n'est plus utilisé. Les hôtes libérés ne peuvent pas être réutilisés.
under-assessment	AWS explore un éventuel problème avec l'hôte dédié. Si des mesures doivent être prises, vous êtes averti par e-mail. AWS Management Console Aucune instance ne peut être lancée sur un Hôte dédié dans cet état.
pending	L'Hôte dédié ne peut pas être utilisé le lancement de nouvelles instances . Soit il est en cours de modification afin de prendre en charge plusieurs types d'instances , soit une récupération d'hôte est en cours.
permanent-failure	Une défaillance irrécupérable a été détectée. Vous recevez une notice d'expulsion par l'intermédiaire de vos instances et par e-mail. Vos instances peuvent continuer à s'exécuter. Si vous arrêtez ou mettez fin à toutes les instances d'un hôte dédié présentant cet état, l'hôte AWS est retiré. AWS ne redémarre pas les instances dans cet état. Aucune instance ne peut être lancée sur un Hôtes dédiés dans cet état.
released-permanent-failure	AWS libère définitivement les hôtes dédiés en panne et sur lesquels aucune instance n'est en cours d'exécution. L'ID de l'Hôte dédié ne peut plus être utilisé.

Créer des versions d'Hôtes dédiés

Pour pouvoir libérer l'Hôte dédié, vous devez arrêter toutes les instances exécutées sur ce dernier. Ces instances peuvent être migrées vers un autre Hôtes dédiés de votre compte afin que vous puissiez continuer à les utiliser. Ces étapes ne concernent que les Hôtes dédiés à la demande.

Vous pouvez libérer un Hôte dédié à l'aide des méthodes suivantes.

Console

Pour libérer un Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.

3. Sur la page Hôtes dédiés, sélectionnez le Hôte dédié à libérer.
4. Sélectionnez Actions, puis Libérer des hôtes.
5. Choisissez Libérer pour confirmer.

AWS CLI

Pour libérer un Hôte dédié

Utilisez la commande [release-hosts](#) AWS CLI .

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

Pour libérer un Hôte dédié

Utilisez la [Remove-EC2Hosts](#) AWS Tools for Windows PowerShell commande.

```
PS C:\> Remove-EC2Hosts -HostId h-012a3456b7890cdef
```

Une fois que vous avez libéré un Hôte dédié, vous ne pouvez plus réutiliser le même hôte ou ID d'hôte et la facturation à la demande pour cet hôte cesse. L'état de l'Hôte dédié devient `released` et vous ne pouvez plus lancer aucune instance sur cet hôte.

Note

Si vous avez récemment libéré des Hôtes dédiés, il peut s'écouler un peu de temps avant qu'ils cessent d'être comptabilisés dans le cadre de votre limite. Pendant ce temps, vous pouvez recevoir des erreurs `LimitExceeded` lorsque vous essayez d'allouer de nouveaux Hôtes dédiés. Dans ce cas, réessayez d'allouer ces nouveaux hôtes après quelques minutes.

Les instances qui ont été arrêtées peuvent toujours être utilisées et sont répertoriées à la page Instances. Elles conservent leur paramètre de location `host`.

Acheter des réservations d'hôtes dédiés

Vous pouvez acheter des réservations en utilisant les méthodes suivantes :

Console

Pour acheter des réservations

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Hôtes dédiés, Réservations d'hôtes dédiés, Purchase Réservation d'hôtes dédiés (Acheter un hôte dédié).
3. Sur l'écran Rechercher des offres, procédez comme suit :
 - a. Dans Famille d'instances, sélectionnez la famille d'instances de l'hôte dédié pour lequel vous souhaitez acheter la réservation d'hôte dédié.
 - b. Pour l'option de paiement, sélectionnez et configurez votre option de paiement préférée.
4. Choisissez Suivant.
5. Sélectionnez les hôtes dédiés auxquels associer la réservation d'hôte dédié, puis choisissez Next.
6. (Facultatif) Attribuez des tags à la réservation d'hôte dédié.
7. Vérifiez votre commande et choisissez Acheter.

AWS CLI

Pour acheter des réservations

1. Utilisez la AWS CLI commande [describe-host-reservation-offerings](#) pour répertorier les offres disponibles qui répondent à vos besoins. L'exemple suivant répertorie les offres qui prennent en charge des instances dans la famille d'instances m4 et ont une durée d'un an.

Note

La durée est indiquée en secondes. Une période d'un an comporte 31 536 000 secondes, tandis qu'une période de trois ans comporte 94 608 000 secondes.

```
aws ec2 describe-host-reservation-offerings --filter Name=instance-family,Values=m4 --max-duration 31536000
```

Les deux commandes renvoient une liste d'offres qui correspondent à vos critères de recherche. Notez l'`offeringId` de l'offre à acheter.

2. Utilisez la AWS CLI commande [purchase-host-reservation](#) pour acheter l'offre et fournissez les informations indiquées à l'étape `offeringId` précédente. L'exemple suivant achète la réservation spécifiée et l'associe à un hôte dédié spécifique qui est déjà attribué dans le AWS compte, et il applique une balise avec une clé `purpose` et une valeur `production`.

```
aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --
host-id-set h-013abcd2a00cbd123 --tag-specifications 'ResourceType=host-
reservation,Tags={Key=purpose,Value=production}'
```

PowerShell

Pour acheter des réservations

1. Utilisez la [Get-EC2HostReservationOffering](#) AWS Tools for Windows PowerShell commande pour répertorier les offres disponibles qui répondent à vos besoins. Les exemples suivants répertorient les offres qui prennent en charge des instances dans la famille d'instances m4 et ont une durée d'un an.

Note

La durée est indiquée en secondes. Une période d'un an comporte 31 536 000 secondes, tandis qu'une période de trois ans comporte 94 608 000 secondes.

```
PS C:\> $filter = @{Name="instance-family"; Value="m4"}
```

```
PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
```

Les deux commandes renvoient une liste d'offres qui correspondent à vos critères de recherche. Notez l'`offeringId` de l'offre à acheter.

2. Utilisez la [New-EC2HostReservation](#) AWS Tools for Windows PowerShell commande pour acheter l'offre et fournissez les informations `offeringId` indiquées à l'étape précédente.

L'exemple suivant achète la réservation spécifiée et l'associe à un hôte dédié spécifique déjà attribué dans le AWS compte.

```
PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -  
HostIdSet h-013abcd2a00cbd123
```

Afficher les réservations d'Hôte dédié

Vous pouvez afficher des informations sur les Hôtes dédiés associés à votre réservation, en particulier :

- Durée de la réservation
- Options de paiement
- Dates de début et de fin

Vous pouvez consulter les détails de vos réservations d'Hôte dédié en utilisant les méthodes suivantes.

Console

Pour voir les détails d'une réservation d'Hôte dédié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Hôtes dédiés dans le volet de navigation.
3. Sur la page Hôtes dédiés, choisissez Réservations d'Hôte dédié et sélectionnez la réservation dans la liste fournie.
4. Sélectionnez Détails pour en savoir plus sur la réservation.
5. Choisissez Hôtes pour en savoir plus sur les Hôtes dédiés auquel la réservation est associée.

AWS CLI

Pour voir les détails d'une réservation d'Hôte dédié

Utilisez la commande [describe-host-reservations](#) AWS CLI .

```
aws ec2 describe-host-reservations
```

PowerShell

Pour voir les détails d'une réservation d'Hôte dédié

Utilisez la [Get-EC2HostReservation](#) AWS Tools for Windows PowerShell commande.

```
PS C:\> Get-EC2HostReservation
```

Baliser les réservations d'hôtes dédiés

Vous pouvez allouer des balises personnalisées à vos réservations d'hôtes dédiés pour classer celles-ci de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Cela vous aide à trouver rapidement un Réservation d'hôtes dédiés spécifique en fonction des balises personnalisées que vous lui avez attribuées.

Vous pouvez attribuer des balises à un Réservation d'hôtes dédiés uniquement à l'aide des outils de ligne de commande.

AWS CLI

Pour attribuer des balises à un Réservation d'hôtes dédiés

Utilisez la commande [create-tags](#) AWS CLI .

```
aws ec2 create-tags --resources hr-1234563a4ffc669ae --tags Key=Owner,Value=TeamA
```

PowerShell

Pour attribuer des balises à un Réservation d'hôtes dédiés

Utilisez la [New-EC2Tag](#) AWS Tools for Windows PowerShell commande.

La commande New-EC2Tag nécessite un paramètre Tag, qui spécifie la paire clé-valeur à utiliser pour la balise d'Réservation d'hôtes dédiés. Les commandes suivantes créent le paramètre Tag :

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag  
PS C:\> $tag.Key = "Owner"  
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource hr-1234563a4ffc669ae -Tag $tag
```

Utiliser des Hôtes dédiés partagés

Le partage d'hôtes dédiés permet aux propriétaires d'hôtes dédiés de partager leurs hôtes dédiés avec d'autres AWS comptes ou au sein d'une AWS organisation. Cela vous permet de créer et de gérer des hôtes dédiés de manière centralisée, et de partager l'hôte dédié entre plusieurs AWS comptes ou au sein de votre AWS organisation.

Dans ce modèle, le AWS compte propriétaire de l'hôte dédié (propriétaire) le partage avec d'autres AWS comptes (consommateurs). Les consommateurs peuvent lancer des instances sur des Hôtes dédiés partagés avec eux comme ils le feraient sur des Hôtes dédiés qu'ils alloueraient dans leur propre compte. Le propriétaire est responsable de la gestion de l'Hôte dédié et des instances lancées sur celui-ci. Les propriétaires ne peuvent pas modifier les instances que les consommateurs lancent sur les Hôtes dédiés partagés. Les consommateurs sont responsables de la gestion des instances qu'ils lancent sur les Hôtes dédiés partagés avec eux. Les consommateurs ne peuvent ni afficher ni modifier les instances détenues par d'autres consommateurs ou par le propriétaire de l'Hôte dédié, et ils ne peuvent pas modifier les Hôtes dédiés qui sont partagés avec eux.

Un propriétaire d'Hôte dédié peut partager un Hôte dédié avec :

- AWS Comptes spécifiques à l'intérieur ou à l'extérieur de son AWS organisation
- Une unité organisationnelle au sein de son AWS organisation
- Toute son AWS organisation

Table des matières

- [Conditions préalables au partage d'Hôtes dédiés](#)
- [Limites pour le partage des Hôte dédiés](#)
- [Services connexes](#)
- [Partager sur plusieurs zones de disponibilité](#)
- [Partager un Hôte dédié](#)
- [Départager un Hôte dédié partagé](#)
- [Identifier un Hôte dédié partagé](#)
- [Afficher les instances en cours d'exécution sur un Hôte dédié partagé](#)
- [Autorisations relatives à un Hôte dédié partagé](#)
- [Facturation et mesures](#)
- [Limites Hôte dédié](#)

- [Récupération d'hôte et partage d'Hôte dédié](#)

Conditions préalables au partage d'Hôtes dédiés

- Pour partager un hôte dédié, vous devez le posséder dans votre AWS compte. Vous ne pouvez pas partager un hôte dédié qui a été partagé avec vous.
- Pour partager un hôte dédié avec votre AWS organisation ou une unité organisationnelle de votre AWS organisation, vous devez activer le partage avec AWS Organizations. Pour plus d'informations, consultez [Activation du partage avec AWS Organizations](#) dans le Guide de l'utilisateur AWS RAM .

Limites pour le partage des Hôte dédiés

Vous ne pouvez pas partager les Hôtes dédiés qui ont été alloués pour les types d'instance suivants : `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` et `u-24tb1.metal`.

Services connexes

AWS Resource Access Manager

Le partage d'hôtes dédiés s'intègre à AWS Resource Access Manager (AWS RAM). AWS RAM est un service qui vous permet de partager vos AWS ressources avec n'importe quel AWS compte ou via AWS Organizations. Avec AWS RAM, vous partagez les ressources que vous possédez en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent être AWS des comptes individuels, des unités organisationnelles ou l'ensemble d'une organisation AWS Organizations.

Pour plus d'informations AWS RAM, consultez le [guide de AWS RAM l'utilisateur](#).

Partager sur plusieurs zones de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte. Cela peut entraîner des différences de nom de zone de disponibilité entre les comptes. Par exemple, il est possible que la zone `us-east-1a` de disponibilité de votre AWS compte ne soit pas la même que celle `us-east-1a` d'un autre AWS compte.

Pour identifier l'emplacement de vos Hôtes dédiés par rapport à vos comptes, vous devez utiliser l'ID de zone de disponibilité. L'ID de zone de disponibilité est un identifiant unique et cohérent pour

une zone de disponibilité sur tous les AWS comptes. Par exemple, use1-az1 est un ID de zone de disponibilité pour la région us-east-1, qui correspond au même emplacement dans chaque compte AWS .

Pour afficher les ID des zones de disponibilité dans votre compte

1. Ouvrez la AWS RAM console à l'[adresse https://console.aws.amazon.com/ram](https://console.aws.amazon.com/ram).
2. Les ID de zone de disponibilité pour la région actuelle sont affichés dans le volet Your AZ ID (Votre ID de zone de disponibilité) dans la partie droite de l'écran.

Partager un Hôte dédié

Lorsqu'un propriétaire partage un Hôte dédié, il permet aux consommateurs de lancer des instances sur l'hôte. Les consommateurs peuvent lancer autant d'instances sur l'hôte partagé que sa capacité disponible le permet.

Important

Notez que vous êtes responsable de vous assurer que vous disposez des droits de licence appropriés pour partager les licences BYOL sur votre Hôtes dédiés.

Si vous partagez un Hôte dédié en ayant activé le placement automatique, gardez ce qui suit à l'esprit car cela pourrait conduire à une utilisation involontaire de l'Hôte dédié :

- Si les consommateurs lancent des instances avec location d'Hôte dédié et qu'ils n'ont pas de capacité sur un Hôte dédié qu'ils possèdent dans leur compte, l'instance est automatiquement lancée sur l'Hôte dédié partagé.

Pour partager un Hôte dédié, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une AWS RAM ressource qui vous permet de partager vos ressources entre différents AWS comptes. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Vous pouvez ajouter l'Hôte dédié à une ressource existante ou l'ajouter à un nouveau partage de ressources.

Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, les clients de votre organisation ont automatiquement accès à l'hôte dédié

partagé. Dans le cas contraire, les consommateurs reçoivent une invitation à rejoindre le partage de ressources et bénéficient d'un accès à l'Hôte dédié partagé après avoir accepté l'invitation.

Note

Après avoir partagé un Hôte dédié, les consommateurs peuvent y avoir accès en quelques minutes.

Vous pouvez partager un Hôte dédié que vous possédez à l'aide de l'une des méthodes suivantes.

Amazon EC2 console

Pour partager un Hôte dédié qui vous appartient à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Choisissez le Hôte dédié à partager, puis choisissez Actions, Partager l'hôte.
4. Sélectionnez le partage de ressources auquel vous souhaitez ajouter le Hôte dédié, puis choisissez Partager l'hôte.

Les consommateurs peuvent avoir accès à l'hôte partagé en quelques minutes.

AWS RAM console

Pour partager un hôte dédié dont vous êtes propriétaire à l'aide de la AWS RAM console

Consultez [Création d'un partage de ressources](#) dans le Guide de l'utilisateur AWS RAM .

AWS CLI

Pour partager un hôte dédié dont vous êtes le propriétaire à l'aide du AWS CLI

Utilisez la commande [create-resource-share](#).

Départager un Hôte dédié partagé

Le propriétaire d'un Hôte dédié peut annuler le partage d'un Hôte dédié partagé à tout moment. Lorsque vous annulez le partage d'un Hôte dédié partagé, les règles suivantes s'appliquent :

- Les consommateurs avec qui l'Hôte dédié a été partagé ne peuvent plus lancer de nouvelles instances sur celui-ci.
- Les instances appartenant à des consommateurs qui s'exécutaient sur l'Hôte dédié au moment de l'annulation du partage continuent de s'exécuter, mais sont programmées pour être [mises hors service](#). Les consommateurs reçoivent des notifications de mise hors service pour les instances, et disposent de deux semaines pour prendre les mesures nécessaires. Toutefois, si l'Hôte dédié est à nouveau partagé avec le consommateur au cours de la période de préavis de mise hors service, les mises hors service d'instance sont annulées.

Pour annuler le partage d'un Hôte dédié partagé qui vous appartient, vous devez le supprimer du partage de ressources. Pour ce faire, utilisez l'une des méthodes suivantes :

Amazon EC2 console

Pour annuler le partage d'un Hôte dédié partagé qui vous appartient à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Choisissez le Hôte dédié dont vous voulez annuler le partage et choisissez l'onglet Partage.
4. L'onglet Partage affiche la liste des partages de ressources auxquels le Hôte dédié a été ajouté. Sélectionnez le partage de ressources duquel vous souhaitez supprimer le Hôte dédié, puis choisissez Supprimer l'hôte du partage de ressources.

AWS RAM console

Pour annuler le partage d'un hôte dédié partagé qui vous appartient à l'aide de la console AWS RAM

Consultez [Mise à jour d'un partage de ressources](#) dans le Guide de l'utilisateur AWS RAM .

Command line

Pour annuler le partage d'un hôte dédié partagé dont vous êtes le propriétaire à l'aide du AWS CLI

Utilisez la commande [disassociate-resource-share](#).

Identifier un Hôte dédié partagé

Les propriétaires et les consommateurs peuvent identifier les Hôtes dédiés partagés à l'aide de l'une des méthodes suivantes.

Amazon EC2 console

Pour identifier un Hôte dédié partagé à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés. L'écran affiche la liste des Hôtes dédiés qui vous appartiennent et des Hôtes dédiés qui sont partagés avec vous. La colonne Propriétaire affiche l'ID du compte AWS du propriétaire de l'hôte dédié.

Command line

Pour identifier un hôte dédié partagé à l'aide du AWS CLI

Utilisez la commande [describe-hosts](#). La commande renvoie les Hôtes dédiés qui vous appartiennent et les Hôtes dédiés qui sont partagés avec vous.

Afficher les instances en cours d'exécution sur un Hôte dédié partagé

Les propriétaires et les consommateurs peuvent afficher les instances s'exécutant sur un Hôte dédié partagé à tout moment à l'aide de l'une des méthodes suivantes.

Amazon EC2 console

Pour afficher les instances s'exécutant sur un Hôte dédié partagé à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'Hôte dédié pour lequel afficher les instances et choisissez Instances. L'onglet répertorie les instances qui s'exécutent sur l'hôte. Les propriétaires voient toutes les instances s'exécutant sur l'hôte, y compris les instances lancées par les consommateurs. Les consommateurs ne voient que les instances en cours d'exécution qu'ils ont lancées sur l'hôte. La colonne Propriétaire affiche l'ID de compte AWS du compte qui a lancé l'instance.

Command line

Pour afficher les instances s'exécutant sur un hôte dédié partagé à l'aide de la AWS CLI

Utilisez la commande [describe-hosts](#). La commande renvoie les instances s'exécutant sur chaque Hôte dédié. Les propriétaires voient toutes les instances s'exécutant sur l'hôte. Les consommateurs ne voient que les instances en cours d'exécution qu'ils ont lancées sur les hôtes partagés. InstanceOwnerId affiche l'ID de compte AWS du propriétaire de l'instance.

Autorisations relatives à un Hôte dédié partagé

Autorisations accordées aux propriétaires

Les propriétaires sont responsables de la gestion de leurs Hôtes dédiés partagés et des instances qu'ils lancent sur eux. Les propriétaires peuvent afficher toutes les instances s'exécutant sur l'Hôte dédié partagé, y compris celles lancées par les consommateurs. Toutefois, les propriétaires ne peuvent effectuer aucune action sur les instances en cours d'exécution lancées par les consommateurs.

Autorisations accordées aux consommateurs

Les consommateurs sont responsables de la gestion des instances qu'ils lancent sur un Hôte dédié partagé. Les consommateurs ne peuvent en aucun cas modifier l'Hôte dédié partagé. Ils ne peuvent pas non plus afficher ou modifier les instances qui ont été lancées par d'autres consommateurs ou par le propriétaire de l'Hôte dédié.

Facturation et mesures

Le partage d'Hôtes dédiés n'entraîne pas de frais supplémentaires.

Les propriétaires sont facturés pour les Hôtes dédiés qu'ils partagent. Les consommateurs ne sont pas facturés pour les instances qu'ils lancent sur des Hôtes dédiés partagés.

Les réservations d'hôtes dédiés continuent à fournir des remises de facturation pour les Hôtes dédiés partagés. Seuls les propriétaires d'Hôte dédié peuvent acheter des réservations d'hôtes dédiés pour les Hôtes dédiés partagés qu'ils possèdent.

Limites Hôte dédié

Les Hôtes dédiés partagés sont uniquement pris en compte dans les limites d'Hôtes dédiés du propriétaire. Les limites d'Hôtes dédiés du consommateur ne sont pas affectées par les Hôtes dédiés

qui ont été partagés avec lui. De même, les instances que les consommateurs lancent sur les Hôtes dédiés partagés ne sont pas pris en compte dans leurs limites d'instance.

Récupération d'hôte et partage d'Hôte dédié

La récupération d'hôte permet de récupérer les instances lancées par le propriétaire d'un Hôte dédié et par les consommateurs avec qui ce dernier a été partagé. L'Hôte dédié de remplacement est alloué au compte du propriétaire. Il est ajouté aux mêmes partages de ressources que l'Hôte dédié d'origine, et il est partagé avec les mêmes consommateurs.

Pour plus d'informations, consultez [Restauration de l'hôte](#).

Hôtes dédiés sur AWS Outposts

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructure, les services, les API et les outils à vos locaux. En fournissant un accès local à l'infrastructure AWS gérée, vous AWS Outposts pouvez créer et exécuter des applications sur site en utilisant les mêmes interfaces de programmation que dans AWS les régions, tout en utilisant les ressources de calcul et de stockage locales pour réduire la latence et les besoins de traitement des données locaux.

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région.

Vous pouvez allouer des hôtes dédiés à des Outposts que vous possédez dans votre compte. Cela vous permet d'apporter plus facilement vos licences logicielles existantes et vos charges de travail nécessitant un serveur physique dédié à AWS Outposts. Vous pouvez également cibler des actifs matériels spécifiques sur un Outpost afin de minimiser la latence entre vos charges de travail.

Les hôtes dédiés vous permettent d'utiliser vos licences logicielles éligibles sur Amazon EC2, de sorte que vous bénéficiez de la flexibilité et de la rentabilité de l'utilisation de vos propres licences. D'autres licences logicielles liées à des machines virtuelles, des sockets ou des cœurs physiques peuvent également être utilisées sur des hôtes dédiés, sous réserve de leurs conditions de licence. Bien que les Outposts aient toujours été des environnements à locataire unique éligibles pour des charges de travail BYOL, les hôtes dédiés vous permettent de limiter les licences nécessaires à un seul hôte plutôt qu'à l'ensemble du déploiement Outpost.

En outre, l'utilisation d'hôtes dédiés sur un Outpost vous offre une plus grande flexibilité dans le déploiement de type d'instance et un contrôle plus précis du placement des instances. Vous pouvez cibler un hôte spécifique pour les lancements d'instances et utiliser l'affinité de l'hôte pour garantir que l'instance s'exécute toujours sur cet hôte, ou vous pouvez utiliser le placement automatique pour

lancer une instance sur n'importe quel hôte disponible disposant de configurations et de capacités disponibles correspondantes.

Table des matières

- [Prérequis](#)
- [Fonctionnalités prises en charge](#)
- [Considérations](#)
- [Allouer et utiliser un hôte dédié sur Outpost](#)

Prérequis

Vous devez avoir un outpost installé sur votre site. Pour plus d'informations, consultez [Créer un outpost et commander une capacité outpost](#) dans le Guide de l'utilisateur AWS Outposts .

Fonctionnalités prises en charge

- Les familles d'instances suivantes sont prises en charge : C5, M5, R5, C5d, M5d, R5d, G4dn et i3en.
- Les hôtes dédiés sur Outposts peuvent être configurés pour prendre en charge plusieurs tailles d'instance. La prise en charge de plusieurs tailles d'instance est disponible pour les familles d'instances suivantes : C5, M5, R5, C5d, M5d, et R5d. Pour plus d'informations, consultez [Configurations de capacité d'instance](#).
- Les hôtes dédiés sur Outposts prennent en charge le placement automatique et les lancements d'instances ciblées. Pour plus d'informations, consultez [Comprendre le placement automatique et l'affinité](#).
- Les hôtes dédiés sur Outposts prennent en charge l'affinité de l'hôte. Pour plus d'informations, consultez [Comprendre le placement automatique et l'affinité](#).
- Les hôtes dédiés sur Outposts prennent en charge le partage avec AWS RAM. Pour plus d'informations, consultez [Utiliser des Hôtes dédiés partagés](#).

Considérations

- Les réservations d'hôtes dédiés ne sont pas prises en charge sur Outposts.
- Hébergez des groupes de ressources AWS License Manager qui ne sont pas pris en charge sur Outposts.
- Les hôtes dédiés sur Outposts ne prennent pas en charge les instances T3 burstable.

- Les hôtes dédiés sur Outposts ne prennent pas en charge la récupération de l'hôte.
- La restauration automatique simplifiée n'est pas prise en charge pour les instances dotées d'une location d'hôte dédié sur Outposts.

Allouer et utiliser un hôte dédié sur Outpost

Vous allouez et utilisez des hôtes dédiés sur des Outposts de la même manière que pour les hôtes dédiés dans une Région AWS .

Prérequis

Créez un sous-réseau sur l'outpost. Pour plus d'informations, consultez [Créer un sous-réseau](#) dans le Guide de l'utilisateur AWS Outposts .

Pour allouer un hôte dédié à un Outpost, utilisez l'une des méthodes suivantes :

AWS Outposts console

1. Ouvrez la AWS Outposts console à l'[adresse https://console.aws.amazon.com/outposts/](https://console.aws.amazon.com/outposts/).
2. Dans le panneau de navigation, choisissez Outposts. Sélectionnez l'Outpost, puis choisissez Actions, Allocate Dedicated Host (Allouer un hôte dédié).
3. Configurez l'hôte dédié selon les besoins. Pour plus d'informations, consultez [Allouer des Hôtes dédiés](#).

Note

La Availability Zone (Zone de disponibilité) et l'Outpost ARN (ARN d'Outpost) doivent être préremplis avec la zone de disponibilité et l'ARN de l'avant-poste sélectionné.

4. Choisissez Allouer.

Amazon EC2 console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Hôtes dédiés, puis Allouer un Hôte dédié.
3. Pour Zone de disponibilité, sélectionnez la zone de disponibilité associée à l'avant-poste.
4. Pour ARN d'Outpost, entrez l'ARN de l'avant-poste.

5. Pour cibler des actifs matériels spécifiques sur l'Outpost, pour Cibler des actifs matériels spécifiques sur l'Outpost, sélectionnez Activer. Pour chaque actif matériel à cibler, sélectionnez Ajouter un identifiant d'actif, puis saisissez l'identifiant d'actif matériel.

 Note

La valeur que vous indiquez pour Quantité doit être égale au nombre d'identifiants d'actifs que vous indiquez. Par exemple, si vous indiquez 3 identifiants d'actifs, Quantité doit également être égale à 3.

6. Configurez les paramètres de l'hôte dédié restant selon les besoins. Pour plus d'informations, consultez [Allouer des Hôtes dédiés](#).
7. Choisissez Allouer.

AWS CLI

Utilisez la commande [allocate-hosts](#) AWS CLI . Pour `--availability-zone`, spécifiez la zone de disponibilité associée à l'avant-poste. Pour `--outpost-arn`, spécifiez l'ARN de l'avant-poste. En option, pour `--asset-ids`, indiquez les identifiants des actifs matériels de l'Outpost à cibler.

```
aws ec2 allocate-hosts --availability-zone "us-east-1a" --outpost-arn  
"arn:aws:outposts:us-east-1a:111122223333:outpost/op-4fe3dc21baEXAMPLE" --asset-  
ids asset_id --instance-family "m5" --auto-placement "off" --quantity 1
```

Pour lancer une instance dans un Hôte dédié sur un avant-poste

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés. Sélectionnez l'hôte dédié que vous avez alloué à l'étape précédente et choisissez Actions, Launch instance onto host (Lancer une instance sur l'hôte).
3. Configurez l'instance selon les besoins, puis lancez l'instance. Pour plus d'informations, consultez [Lancer des instances sur un Hôte dédié](#).

Restoration de l'hôte

La fonction de récupération automatique de l'hôte dédiée redémarre vos instances sur un nouvel hôte de remplacement lorsque certaines conditions problématiques sont détectées sur votre hôte dédié.

La fonction de récupération de l'hôte permet de réduire les interventions manuelles et de diminuer la charge de travail opérationnelle en cas d'incident inattendu lié à l'alimentation système ou à des événements de connectivité réseau sur un hôte dédié. Les autres problèmes liés à l'hôte dédié nécessiteront une intervention manuelle pour être résolus.

Table des matières

- [Notions de base de la récupération de l'hôte](#)
- [Types d'instance pris en charge](#)
- [Configurer la récupération de l'hôte](#)
- [États de la récupération de l'hôte](#)
- [Récupérer manuellement les instances non prises en charge](#)
- [Services connexes](#)
- [Tarification](#)

Notions de base de la récupération de l'hôte

Les hôtes dédiés et la fonction de récupération des groupes de ressource d'hôtes font intervenir des surveillances de l'état au niveau de l'hôte pour évaluer la disponibilité de l'hôte dédié et détecter les pannes système sous-jacentes. Le type de défaillance de l'hôte dédié détermine si la récupération automatique de l'hôte dédié est possible. Voici quelques exemples de problèmes pouvant entraîner l'échec des vérifications de l'état au niveau de l'hôte :

- Perte de connectivité réseau
- Perte d'alimentation système
- Problèmes logiciels ou matériels sur l'hôte physique

Important

La récupération automatique de l'hôte dédié n'a pas lieu lorsque la mise hors service de l'hôte est prévue.

Récupération automatique de l'hôte dédié

Lorsqu'une panne d'alimentation du système ou de connectivité réseau est détectée sur votre hôte dédié, la restauration automatique de l'hôte dédié est lancée et Amazon EC2 alloue automatiquement

un hôte dédié de remplacement dans la même zone de disponibilité que l'hôte dédié d'origine. L'Hôte dédié de remplacement reçoit un nouvel ID d'hôte, mais conserve les mêmes attributs que l'Hôte dédié d'origine, en particulier :

- Zone de disponibilité
- Type d'instance
- Balises
- Paramètres de placement automatique
- Réserve

Une fois l'hôte dédié de remplacement alloué, les instances sont récupérées sur l'hôte dédié de remplacement. Les instances récupérées conservent les mêmes attributs que les instances d'origine, en particulier :

- ID d'instance
- Adresses IP privées
- Adresses IP Elastic
- Pièces jointes de volume EBS
- Toutes les métadonnées d'instance

En outre, l'intégration intégrée à AWS License Manager automatise le suivi et la gestion de vos licences.

 Note

AWS L'intégration de License Manager n'est prise en charge que dans les régions dans lesquelles AWS License Manager est disponible.

Si des instances ont des relations d'affinité avec l'Hôte dédié déficient, les instances récupérées établissent une relation d'affinité avec l'Hôte dédié de remplacement.

Une fois que toutes les instances ont été récupérées sur l'Hôte dédié de remplacement, l'Hôte dédié déficient est libéré et l'Hôte dédié de remplacement devient disponible.

Lorsque la restauration de l'hôte est lancée, le propriétaire du AWS compte est averti par e-mail et par un AWS Health Dashboard événement. Une seconde notification est envoyée une fois la récupération de l'hôte réalisée avec succès.

Si vous utilisez AWS License Manager pour suivre vos licences, AWS License Manager alloue de nouvelles licences à l'hôte dédié de remplacement en fonction des limites de configuration des licences. Si la configuration de la licence comporte des limites strictes qui seront dépassées à la suite de la restauration de l'hôte, le processus de restauration n'est pas autorisé et vous êtes informé de l'échec de la restauration de l'hôte par le biais d'une notification Amazon SNS (si les paramètres de notification ont été configurés pour License AWS Manager). Si la configuration de licence définit des limites flexibles qui seront outrepassées à la suite de la récupération de l'hôte, le processus de récupération est autorisé et vous êtes averti du dépassement de la limite via une notification Amazon SNS. Pour plus d'informations, consultez [Configurations de licences dans License Manager](#) et [Paramètres dans License Manager](#) dans le Guide de l'utilisateur AWS License Manager.

Scénarios sans récupération automatique d'hôte dédié

La récupération automatique de l'hôte dédié n'a pas lieu lorsque la mise hors service de l'hôte est prévue. Vous recevrez une notification de retrait lors d'un CloudWatch événement Amazon AWS Health Dashboard, et l'adresse e-mail du propriétaire du AWS compte recevra un message concernant la défaillance de l'hôte dédié. Suivez les étapes correctives décrites dans la notification de mise hors service dans le temps imparti pour récupérer manuellement les instances sur l'hôte qui est mis hors service.

Les instances arrêtées ne sont pas récupérées sur l'Hôte dédié de remplacement. Si vous tentez de démarrer une instance arrêtée qui cible l'Hôte dédié déficient, son démarrage échoue. Nous vous recommandons de modifier l'instance arrêtée afin qu'elle cible un autre Hôte dédié ou de la lancer sur tout Hôte dédié disponible ayant des caractéristiques de configuration et de remplacement automatique correspondantes.

Les instances avec stockage d'instance ne sont pas récupérées sur l'Hôte dédié de remplacement. Afin de remédier à ce problème, l'Hôte dédié déficient est marqué comme devant être mis hors service et vous recevez une notification de mise hors service une fois la récupération de l'hôte terminée. Suivez les étapes correctives décrites dans la notification de mise hors service dans le temps imparti pour récupérer manuellement les instances restantes sur l'Hôte dédié déficient.

Types d'instance pris en charge

La restauration de l'hôte est prise en charge pour les familles d'instances suivantes : A1, C3, C4, C5, C5n, C6a, C6g, C6i, Inf1, G3, G5g, M3, M4, M5, M5n, M5zn, M6a, M6g, M6i, P2, P3, R3, R4, R5, R5b, R5n, R6g, R6i, T3, X1, X1e, X2iezn, u-6tb1, u-9tb1, u-12tb1, u-18tb1 et u-24tb1.

Pour récupérer des instances qui ne sont pas prises en charge, consultez [Récupérer manuellement les instances non prises en charge](#).

Note

La récupération automatique de l'hôte dédié pour les types d'instance métalliques pris en charge prendra plus de temps à détecter et à récupérer que pour les types d'instance non métalliques.

Configurer la récupération de l'hôte

Vous pouvez configurer la restauration de l'hôte au moment de l'allocation de l'hôte dédié ou après l'allocation à l'aide de la console Amazon EC2 ou (AWS Command Line Interface CLI).

Table des matières

- [Activer la restauration de l'hôte](#)
- [Désactiver la restauration de l'hôte](#)
- [Afficher la configuration de récupération de l'hôte](#)

Activer la restauration de l'hôte

Vous pouvez activer la récupération de l'hôte au moment de l'allocation de l'Hôte dédié ou après l'allocation.

Pour plus d'informations sur l'activation de la récupération de l'hôte au moment de l'allocation de l'Hôte dédié, consultez [Allouer des Hôtes dédiés](#).

Pour activer la récupération de l'hôte après l'allocation à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.

3. Sélectionnez l'Hôte dédié pour lequel vous souhaitez activer la fonction de récupération de l'hôte, puis choisissez Actions, Modify Host Recovery (Modifier la récupération de l'hôte).
4. Pour Host recovery (Récupération de l'hôte), choisissez Enable (Activer), puis Save (Enregistrer).

Pour activer la restauration de l'hôte après allocation à l'aide du AWS CLI

Utilisez la commande [modify-hosts](#) et spécifiez le paramètre `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery on --host-ids h-012a3456b7890cdef
```

Désactiver la restauration de l'hôte

Vous pouvez désactiver la récupération de l'hôte à tout moment après l'allocation de l'Hôte dédié.

Pour désactiver la récupération de l'hôte après l'allocation à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'Hôte dédié pour lequel vous souhaitez désactiver la fonction de récupération de l'hôte, puis choisissez Actions, Modify Host Recovery (Modifier la récupération de l'hôte).
4. Pour Host recovery (Récupération de l'hôte), choisissez Disable (Désactiver), puis Save (Enregistrer).

Pour désactiver la restauration de l'hôte après l'allocation à l'aide du AWS CLI

Utilisez la commande [modify-hosts](#) et spécifiez le paramètre `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery off --host-ids h-012a3456b7890cdef
```

Afficher la configuration de récupération de l'hôte

Vous pouvez afficher la configuration de récupération de l'hôte d'un Hôte dédié à tout moment.

Pour afficher la configuration de récupération de l'hôte d'un Hôte dédié à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'Hôte dédié, puis, dans l'onglet Description, passez en revue le champ Host Recovery (Récupération de l'hôte).

Pour afficher la configuration de récupération de l'hôte d'un hôte dédié à l'aide de la AWS CLI

Utilisez la commande [describe-hosts](#).

```
$ aws ec2 describe-hosts --host-ids h-012a3456b7890cdef
```

L'élément de réponse `HostRecovery` indique si la récupération de l'hôte est activée ou désactivée.

États de la récupération de l'hôte

Lorsqu'une déficience d'Hôte dédié est détectée, l'Hôte dédié déficient passe à l'état `under-assessment` et toutes les instances passent à l'état `impaired`. Vous ne pouvez pas lancer des instances sur l'Hôte dédié déficient tant qu'il est à l'état `under-assessment`.

Une fois l'Hôte dédié de remplacement alloué, il passe à l'état `pending`. Il reste dans cet état jusqu'à ce que le processus de récupération de l'hôte soit terminé. Vous ne pouvez pas lancer des instances sur l'Hôte dédié de remplacement tant qu'il est à l'état `pending`. Les instances récupérées situées sur l'Hôte dédié de remplacement restent à l'état `impaired` durant le processus de récupération.

Une fois la récupération de l'hôte terminée, l'Hôte dédié de remplacement passe à l'état `available` et les instances récupérées repassent à l'état `running`. Vous pouvez lancer des instances sur l'Hôte dédié de remplacement une fois qu'il est à l'état `available`. L'Hôte dédié déficient d'origine est libéré de façon permanente et il passe à l'état `released-permanent-failure`.

Si l'Hôte dédié déficient possède des instances qui ne prennent pas en charge la récupération de l'hôte, telles que les instances comportant des volumes basés sur le stockage d'instances, l'Hôte dédié n'est pas libéré. Il est marqué comme devant être mis hors service et passe à l'état `permanent-failure`.

Récupérer manuellement les instances non prises en charge

La fonction de récupération de l'hôte ne prend pas en charge la récupération des instances qui utilisent des volumes de stockage d'instances. Suivez les instructions ci-après pour récupérer manuellement les instances qui n'ont pas pu être récupérées automatiquement.

⚠ Warning

Les données stockées sur des volumes de stockage d'instances sont perdues lorsqu'une instance est arrêtée, mise en veille prolongée ou résiliée. Ceci inclut les volumes de stockage d'instances attachés à une instance ayant un volume EBS comme périphérique racine. Pour protéger les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent avant l'arrêt ou la résiliation de l'instance.

Récupérer manuellement les instances basées sur EBS

Pour les instances basées sur des volumes EBS qui n'ont pas pu être récupérées automatiquement, nous vous recommandons de les arrêter puis de les redémarrer manuellement afin de les récupérer sur un nouvel Hôte dédié. Pour plus d'informations sur l'arrêt de votre instance, ainsi que sur les changements apportés à la configuration de votre instance lorsque celle-ci est arrêtée, consultez [Arrêtez et démarrez les instances Amazon EC2](#).

Récupérer manuellement les instances basées sur le stockage d'instances

Pour les instances basées sur le stockage d'instances qui n'ont pas pu être récupérées automatiquement, nous vous recommandons de procéder comme suit :

1. Lancez une instance de remplacement sur un nouvel Hôte dédié à partir de votre AMI la plus récente.
2. Migrez toutes les données nécessaires vers l'instance de remplacement.
3. Résiliez l'instance d'origine sur l'Hôte dédié déficient.

Services connexes

Hôte dédié intègre les services suivants :

- AWS License Manager : assure le suivi des licences sur vos hôtes dédiés Amazon EC2 (pris en charge uniquement dans les régions dans lesquelles License AWS Manager est disponible). Pour plus d'informations, consultez le [Guide de l'utilisateur AWS License Manager](#).

Tarification

Il n'y a pas de facturation supplémentaire pour l'utilisation de la fonction de récupération de l'hôte, mais les frais habituellement appliqués pour l'Hôte dédié vous seront facturés. Pour plus d'informations, consultez [Tarification des hôtes dédiés Amazon EC2](#).

Dès que la fonction de récupération de l'hôte est lancée, vous n'êtes plus facturé pour l'Hôte dédié déficient. La facturation relative à l'hôte dédié de remplacement commence uniquement une fois qu'il est passé à l'état `available`.

Si l'Hôte dédié déficient était facturé au tarif à la demande, l'Hôte dédié de remplacement est également facturé au tarif à la demande. Si l'Hôte dédié déficient possédait une Réservation d'hôtes dédiés, elle est transférée à l'Hôte dédié de remplacement.

Maintenance de l'hôte

Dans le cadre de la maintenance de l'hôte, vos instances Amazon EC2 sur l'hôte dédié dégradé sont automatiquement redémarrées sur un hôte dédié de remplacement lors d'un événement de maintenance planifié. Cela permet de réduire les temps d'arrêt des applications et de déléguer à AWS la lourdeur indifférenciée de la maintenance. La maintenance de l'hôte est également effectuée pour la maintenance planifiée et de routine d'Amazon EC2.

La maintenance de l'hôte est prise en charge pour toutes les nouvelles allocations d'hôtes dédiés effectuées via la console Amazon EC2. Pour tout hôte dédié de votre Compte AWS ou pour tout nouvel hôte dédié alloué via l'[AllocateHostsAPI](#), vous pouvez configurer la maintenance de l'hôte pour les hôtes dédiés pris en charge. Pour plus d'informations, consultez [the section called "Configuration de la maintenance de l'hôte"](#).

Table des matières

- [Principes de base de la maintenance des hôtes](#)
- [Maintenance d'hôte versus récupération d'hôte](#)
- [Types d'instance pris en charge](#)
- [Instances sur hôte dédié](#)
- [Configuration de la maintenance de l'hôte](#)
- [Événement de maintenance](#)
- [États de la maintenance de l'hôte](#)

- [Services connexes](#)
- [Tarification](#)

Principes de base de la maintenance des hôtes

Lorsqu'une dégradation est détectée sur un hôte dédié, un nouvel hôte dédié est alloué. La dégradation peut être causée par la dégradation du matériel sous-jacent ou par la détection de certaines conditions problématiques. Vos instances sur l'hôte dédié dégradé sont programmées pour être automatiquement redémarrées sur l'hôte dédié de remplacement.

L'hôte dédié de remplacement reçoit un nouvel ID d'hôte, mais conserve les mêmes attributs que l'hôte dédié d'origine. Ces attributs sont les suivants.

- Paramètres de placement automatique
- Zone de disponibilité
- Réservation
- Affinité de l'hôte
- Paramètres de maintenance de l'hôte
- Paramètres de récupération de l'hôte
- Type d'instance
- Balises

La maintenance de l'hôte est disponible dans tous les Régions AWS cas pour tous les hôtes dédiés pris en charge. Pour plus d'informations sur les hôtes dédiés pour lesquels la maintenance de l'hôte n'est pas prise en charge, consultez [the section called "Limites"](#).

Votre hôte dédié dégradé est libéré une fois que toutes vos instances ont été redémarrées sur un nouvel hôte dédié ou arrêtées. Vous pouvez accéder à vos instances sur l'hôte dédié dégradé avant l'événement de maintenance programmé, mais le lancement d'instances sur l'hôte dédié dégradé n'est pas pris en charge.

Vous pouvez utiliser l'hôte dédié de remplacement pour lancer de nouvelles instances sur l'hôte avant l'événement de maintenance planifié. Toutefois, une partie de la capacité d'instance de l'hôte de remplacement est réservée aux instances qui doivent être migrées depuis l'hôte dégradé. Vous ne pouvez pas lancer de nouvelles instances dans cette capacité réservée. Pour de plus amples informations, consultez [the section called "Instances sur hôte dédié"](#).

Limites

- La maintenance de l'hôte n'est pas prise en charge dans AWS Outposts les zones AWS Local et les zones AWS Wavelength.
- La maintenance des hôtes ne peut pas être activée ou désactivée pour les hôtes déjà présents dans un groupe de ressources hôte. Les hôtes ajoutés à un groupe de ressources hôte conservent leur paramètre de maintenance d'hôte. Pour plus d'informations, consultez [Groupes de ressources hôte](#).
- La maintenance d'hôte n'est prise en charge que sur des types d'instance spécifiques. Pour plus d'informations, consultez [the section called "Types d'instance pris en charge"](#).

Maintenance d'hôte versus récupération d'hôte

Le tableau suivant présente les principales différences entre la récupération d'hôte et la maintenance d'hôte.

	Restoration de l'hôte	Maintenance de l'hôte
Accessibilité	Injoignable	Joignable
État	under-assessment	permanent-failure
Action	La récupération est immédiate	La maintenance est planifiée
Flexibilité de la planification	Ne peut être planifié à nouveau	Peut être planifié à nouveau
Groupe de ressources hôte	Pris en charge	Non pris en charge

Pour plus d'informations sur la restauration de l'hôte, consultez [Restauration de l'hôte](#).

Types d'instance pris en charge

La maintenance de l'hôte est prise en charge pour les familles d'instances suivantes :

- Usage général : A1 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | T3
- Calcul optimisé : C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7g | C7gn | C7i

- Mémoire optimisée : R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7iz | u-12tb1 | u-18tb1 | u-24tb1 | u-3tb1 | u-6tb1 | u-9tb1 | X2iezn
- Calcul accéléré: G3 | G5g | Inf1 | P2 | P3

Instances sur hôte dédié

Amazon EC2 réserve automatiquement de la capacité sur l'hôte de remplacement pour les instances qui seront automatiquement migrées depuis l'hôte dégradé. Amazon EC2 ne réserve pas de capacité sur l'hôte de remplacement pour les instances qui ne peuvent pas être migrées automatiquement, telles que les instances avec des volumes racine de stockage d'instance. La capacité réservée ne peut pas être utilisée pour lancer de nouvelles instances.

Note

La console Amazon EC2 indique la capacité réservée en tant que capacité utilisée. Il peut sembler que les instances s'exécutent à la fois sur l'hôte dégradé et sur l'hôte de remplacement. Toutefois, les instances continueront de fonctionner uniquement sur l'hôte dégradé jusqu'à ce qu'elles soient arrêtées ou qu'elles soient migrées vers la capacité réservée sur l'hôte de remplacement.

Si vous arrêtez manuellement une instance sur l'hôte dégradé qui peut être migrée automatiquement, la capacité réservée à cette instance sur l'hôte de remplacement est libérée et peut être utilisée.

Au cours de l'événement de maintenance planifié, les instances de l'hôte dégradé sont redémarrées et migrées vers la capacité réservée sur l'hôte dédié de remplacement. Les instances migrées conservent les mêmes attributs que ceux de votre hôte dégradé, notamment les suivants.

- Pièces jointes de volume Amazon EBS
- Adresses IP Elastic
- ID d'instance
- Métadonnées de l'instance
- Adresse IP privée

Vous pouvez arrêter et démarrer une instance sur l'hôte dégradé à tout moment avant le début de l'événement de maintenance planifiée. Ce faisant, vous redémarrerez votre instance sur un autre hôte,

et votre instance ne subira pas la maintenance planifiée. Vous devez mettre à jour l'affinité d'hôte de votre instance avec le nouvel hôte sur lequel vous voulez redémarrer votre instance. Si vous arrêtez toutes les instances de l'hôte dégradé avant le lancement de l'événement de maintenance, l'hôte dégradé est libéré et l'événement de maintenance est annulé. Pour plus d'informations, consultez [Arrêtez et démarrez les instances Amazon EC2](#).

Note

Les données d'un volume de stockage d'instances ne sont pas conservées lorsque vous arrêtez et démarrez votre instance.

Les instances dont le périphérique racine est un volume de stockage d'instances sont résiliées après la date de résiliation spécifiée. Toutes les données des volumes de stockage d'instances sont supprimées lorsque les instances sont résiliées. Les instances résiliées sont définitivement supprimées et ne peuvent pas être redémarrées. Pour les instances dont les volumes de stockage d'instances sont le périphérique racine, nous vous recommandons de lancer des instances de remplacement sur un hôte dédié différent en utilisant l'Amazon Machine Image la plus récente, et de migrer toutes les données disponibles vers les instances de remplacement avant la date de résiliation spécifiée. Pour plus d'informations, voir [Mesures à prendre, par exemple, le départ à la retraite](#).

Les instances qui ne peuvent pas être redémarrées automatiquement sont arrêtées après la date spécifiée. Vous pouvez redémarrer ces instances sur un autre hôte. Les instances utilisant un volume Amazon EBS en tant que périphérique racine continuent d'utiliser le même volume Amazon EBS après avoir été démarrées sur un nouvel hôte.

Vous pouvez définir l'ordre de redémarrage des instances en replanifiant l'heure de début d'un redémarrage d'instance sur <https://console.aws.amazon.com/ec2/>.

Configuration de la maintenance de l'hôte

Vous pouvez configurer la maintenance de l'hôte pour tous les hôtes dédiés pris en charge via AWS Management Console ou AWS CLI. Consultez le tableau suivant pour plus de détails.

AWS Management Console

Pour activer la maintenance de l'hôte pour votre hôte dédié à l'aide de AWS Management Console.

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'hôte dédié > Actions > Modifier l'hôte.
4. Sélectionnez Activé dans le champ Maintenance de l'hôte.

Pour désactiver la maintenance de l'hôte pour votre hôte dédié en utilisant la AWS Management Console.

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'hôte dédié > Actions > Modifier l'hôte.
4. Sélectionnez Désactivé dans le champ Maintenance de l'hôte.

Pour afficher la configuration de maintenance de l'hôte d'un hôte dédié à l'aide de la AWS Management Console.

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Hôtes dédiés.
3. Sélectionnez l'Hôte dédié, puis, dans l'onglet Description, passez en revue le champ Maintenance de l'hôte.

AWS CLI

Pour activer ou désactiver la maintenance de l'hôte pour votre nouvel hôte dédié pendant l'allocation en utilisant l' AWS CLI.

Utilisez la commande [allocate-hosts](#).

Activer

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --availability-zone us-east-1b --host-maintenance on
```

Désactiver

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --availability-zone us-east-1b --host-maintenance off
```

Pour activer ou désactiver la maintenance de l'hôte pour votre hôte dédié existant en utilisant l'AWS CLI.

Utilisez la commande [modify-hosts](#).

Activer

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance on --host-ids h-0d123456bbf78910d
```

Désactiver

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance off --host-ids h-0d123456bbf78910d
```

Pour afficher la configuration de maintenance de l'hôte d'un hôte dédié à l'aide de la AWS CLI.

Utilisez la commande [describe-hosts](#).

```
aws ec2 describe-hosts --region us-east-1 --host-ids h-0d123456bbf78910d
```

Note

Si vous désactivez la maintenance de l'hôte, vous recevez une notification par e-mail vous demandant d'expulser l'hôte endommagé et de migrer manuellement vos instances vers un autre hôte dans les 28 jours. Un hôte de remplacement est attribué si vous avez réservé un hôte dédié. Après 28 jours, les instances exécutées sur l'hôte dégradé sont résiliées et l'hôte est libéré automatiquement.

Événement de maintenance

En cas de détection d'une dégradation, un événement de maintenance est planifié 14 jours plus tard, afin de redémarrer vos instances sur un nouvel hôte dédié. Vous recevez une notification par e-mail fournissant des informations sur l'hôte endommagé, l'événement de maintenance planifié et les plages horaires de maintenance. Pour plus d'informations, consultez [Affichage des événements planifiés](#).

Vous pouvez replanifier l'événement de maintenance pour n'importe quel jour jusqu'à sept jours après la date de l'événement planifié. Pour plus d'informations sur la replanification, consultez [Replanification d'un événement planifié](#).

L'événement de maintenance dure généralement quelques minutes. Dans les rares cas d'échec, vous recevez une notification par e-mail vous demandant d'expulser les instances de l'hôte endommagé dans un délai spécifié.

États de la maintenance de l'hôte

Votre hôte dédié est configuré sur l'état `permanent-failure` lorsqu'une dégradation est détectée. Vous ne pouvez pas lancer d'instances sur un hôte dédié dont l'état est `permanent-failure`. À la fin de l'événement de maintenance, l'hôte dégradé est libéré et placé dans l'état `released`, `permanent-failure`.

Après avoir détecté une dégradation sur un hôte dédié et avant de planifier un événement de maintenance, le service de maintenance de l'hôte alloue automatiquement un hôte dédié de remplacement sur votre compte. Cet hôte de remplacement reste en `pending` état jusqu'à ce qu'un événement de maintenance soit planifié. Une fois l'événement de maintenance planifié, l'hôte dédié de remplacement passe à l'`available` état.

Vous pouvez utiliser l'hôte dédié de remplacement pour lancer de nouvelles instances sur l'hôte avant l'événement de maintenance planifié. Toutefois, une partie de la capacité d'instance de l'hôte de remplacement est réservée aux instances qui doivent être migrées depuis l'hôte dégradé. Vous ne pouvez pas lancer de nouvelles instances dans cette capacité réservée. Pour plus d'informations, consultez [the section called "Instances sur hôte dédié"](#).

Services connexes

Dedicated Host s'intègre à AWS License Manager : suit les licences sur vos hôtes dédiés Amazon EC2 (pris en charge uniquement dans les régions dans lesquelles le License AWS Manager est disponible). Pour plus d'informations, consultez le [Guide de l'utilisateur AWS License Manager](#).

Vous devez disposer de suffisamment de licences Compte AWS pour votre nouvel hôte dédié. Les licences associées à votre hôte dégradé sont libérées lorsque l'hôte est libéré après la fin de l'événement de maintenance planifié.

Tarification

Il n'y a pas de facturation supplémentaire pour l'utilisation de la fonction de maintenance de l'hôte, mais les frais habituellement appliqués pour l'Hôte dédié vous seront facturés. Pour plus d'informations, consultez [Tarification des hôtes dédiés Amazon EC2](#).

Dès que la fonction de maintenance de l'hôte est lancée, vous n'êtes plus facturé pour l'Hôte dédié dégradé. La facturation relative à l'hôte dédié de remplacement commence uniquement une fois qu'il est passé à l'état `available`.

Si l'hôte dédié dégradé a été facturé au tarif à la demande, l'hôte dédié de remplacement est également facturé au tarif à la demande. Si l'hôte dédié dégradé avait une réservation d'hôte dédié active, celle-ci est transférée au nouvel hôte dédié.

Suivre les modifications de configuration

Vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration pour les hôtes dédiés, ainsi que pour les instances lancées, arrêtées ou résiliées sur ces hôtes. Vous pouvez utiliser les informations capturées par AWS Config comme source de données pour les rapports d'utilisation des licences.

AWS Config enregistre les informations de configuration pour les hôtes dédiés et les instances individuellement, et associe ces informations par le biais de relations. Il y a trois conditions pour la création de rapports :

- **AWS Config état de l'enregistrement** : lorsque cette option AWS Config est activée, elle enregistre un ou plusieurs types de AWS ressources, notamment des hôtes dédiés et des instances dédiées. Pour capturer les informations requises pour les rapports d'utilisation des licences, vérifiez que les hôtes et les instances sont enregistrés avec les champs suivants.
- **Statut de l'enregistrement de l'hôte** — Lorsque ce paramètre a la valeur `Activé`, les informations de configuration concernant les Hôtes dédiés sont enregistrées.
- **Statut de l'enregistrement de l'instance** : lorsque ce paramètre est défini sur `Activé`, les informations de configuration concernant les Instances dédiées sont enregistrées.

Si l'une de ces trois conditions est désactivée, l'icône du bouton `Edit Config Recording` est rouge. Afin de tirer pleinement profit de cet outil, assurez-vous que les trois méthodes d'enregistrement soient activées. Lorsqu'elles sont toutes les trois activées, l'icône est verte. Pour modifier les paramètres, choisissez `Edit Config Recording`. Vous êtes dirigé vers la AWS Config page de configuration de la AWS Config console, où vous pouvez configurer AWS Config et démarrer l'enregistrement pour vos

hôtes, instances et autres types de ressources pris en charge. Pour plus d'informations, consultez la section [Configuration à AWS Config l'aide de la console](#) dans le guide du AWS Config développeur.

 Note

AWS Config enregistre vos ressources après les avoir découvertes, ce qui peut prendre plusieurs minutes.

Après avoir AWS Config commencé à enregistrer les modifications de configuration de vos hôtes et instances, vous pouvez obtenir l'historique de configuration de tous les hôtes que vous avez alloués ou publiés et de toutes les instances que vous avez lancées, arrêtées ou résiliées. Par exemple, à tout moment dans l'historique de configuration d'un Hôte dédié, vous pouvez rechercher combien d'instances sont lancées sur cet hôte, ainsi que le nombre de sockets et de cœurs sur l'hôte. Pour n'importe laquelle de ces instances, vous pouvez également rechercher l'ID de son Amazon Machine Image (AMI). Vous pouvez utiliser ces informations pour les rapports de licences portant sur vos propres licences logicielles liées au serveur par socket ou par cœur.

Vous pouvez accéder aux historiques de configuration de l'une des façons suivantes :

- En utilisant la AWS Config console. Pour chaque ressource enregistrée, vous pouvez visualiser une page chronologique fournissant une historique des détails de configuration. Pour visualiser cette page, choisissez l'icône grise dans la colonne Chronologie de configuration de la page Hôtes dédiés. Pour plus d'informations, consultez la section [Affichage des détails de configuration dans la AWS Config console](#) dans le guide du AWS Config développeur.
- En exécutant AWS CLI des commandes. Tout d'abord, vous pouvez utiliser la commande [list-discovered-resources](#) pour obtenir une liste des hôtes et des instances. Vous pouvez ensuite utiliser la commande [get-resource-config-history](#) pour obtenir les détails de configuration d'un hôte ou d'une instance pour un intervalle de temps donné. Pour plus d'informations, consultez [Afficher les détails de configuration à l'aide de la CLI](#) dans le Guide du développeur AWS Config .
- En utilisant l' AWS Config API dans vos applications. Tout d'abord, vous pouvez utiliser l'action [ListDiscoveredResources](#) pour obtenir une liste de tous les hôtes et instances. Vous pouvez ensuite utiliser l'[GetResourceConfigHistory](#) action pour obtenir les détails de configuration d'un hôte ou d'une instance pour un intervalle de temps spécifique.

Par exemple, pour obtenir la liste de tous vos hôtes dédiés AWS Config, exécutez une commande CLI telle que la suivante.

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Pour obtenir l'historique de configuration d'un hôte dédié à partir de AWS Config, exécutez une commande CLI telle que la suivante.

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --resource-id i-1234567890abcdef0
```

Pour gérer les AWS Config paramètres à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sur la page Hôtes dédiés, sélectionnez Modifier l'enregistrement de la configuration.
3. Dans la AWS Config console, suivez les étapes indiquées pour activer l'enregistrement. Pour plus d'informations, consultez la section [Configuration à AWS Config l'aide de la console](#).

Pour plus d'informations, consultez la section [Affichage des détails de configuration dans la AWS Config console](#).

Pour activer à AWS Config l'aide de la ligne de commande ou de l'API

- AWS CLI : [affichage des détails de configuration \(AWS CLI\)](#) dans le guide du AWS Config développeur.
- API Amazon EC2 : [GetResourceConfigHistory](#)

Dedicated instances

Par défaut, les instances EC2 s'exécutent sur un matériel de location partagé. Cela signifie que plusieurs AWS comptes peuvent partager le même matériel physique.

Les instances dédiées sont des instances EC2 qui s'exécutent sur du matériel dédié à un seul AWS compte. Cela signifie que les instances dédiées sont physiquement isolées au niveau du matériel hôte des instances appartenant à d'autres instances Comptes AWS, même si ces comptes sont liés à un compte payeur unique. Toutefois, les instances dédiées peuvent partager du matériel avec d'autres instances de la même instance Compte AWS qui ne sont pas des instances dédiées.

Les instances dédiées n'offrent aucune visibilité ni aucun contrôle sur le placement des instances, et elles ne prennent pas en charge l'affinité avec l'hôte. Si vous arrêtez et démarrez une instance

dédiée, elle risque de ne pas s'exécuter sur le même hôte. De même, vous ne pouvez pas cibler un hôte spécifique sur lequel lancer ou exécuter une instance. En outre, les instances dédiées fournissent un support limité pour Bring Your Own License (BYOL).

Si vous avez besoin de visibilité et de contrôle sur le placement des instances et d'un support BYOL plus complet, pensez plutôt à utiliser un hôte dédié. Les instances dédiées et les hôtes dédiés peuvent tous deux être utilisés pour lancer des instances Amazon EC2 sur des serveurs physiques dédiés. Il n'existe pas de différence physique, de sécurité ou de performance entre les instances dédiées et les instances des Hôtes dédiés. Cependant, il existe des différences majeures entre eux. Le tableau suivant met en valeur quelques-unes des principales différences entre les Hôtes dédiés et les instances dédiées :

	Dedicated Host	Dedicated Instance
Serveur physique dédié	Serveur physique avec une capacité d'instance entièrement dédiée à votre utilisation.	Serveur physique dédié à un seul compte client.
Partage de capacité d'instance	Peut partager la capacité de l'instance avec d'autres comptes.	Non pris en charge
Facturation	Facturation par hôte	Facturation par instance
Visibilité des sockets, cœurs et ID d'hôte	Offre une visibilité sur le nombre de sockets et de cœurs physiques	Aucune visibilité
Affinité de l'hôte et de l'instance	Permet de déployer vos instances de façon cohérente sur le même serveur physique au fil du temps	Non pris en charge
Placement ciblé d'instances	Offre une visibilité supplémentaire et un contrôle sur la façon dont les instances sont placées sur un serveur physique	Non pris en charge

	Dedicated Host	Dedicated Instance
Récupération automatique des instances	Pris en charge. Pour plus d'informations, consultez Restauration de l'hôte .	Pris en charge
Bring Your Own License (Licence à fournir)	Pris en charge	Support partiel*
Réserve de capacité	Non pris en charge	Pris en charge

Serveur * Microsoft SQL avec License Mobility via Software Assurance et les licences Windows Virtual Desktop Access (VDA) peuvent être utilisées avec une instance dédiée.

Pour plus d'informations sur les instances dédiées, veuillez consulter la rubrique [Hôtes dédiés](#).

Rubriques

- [Principes de base de Instance dédiée](#)
- [Fonctionnalités prises en charge](#)
- [Limites de instances dédiées](#)
- [Tarification des instances dédiées](#)
- [Travailler avec instances dédiées](#)

Principes de base de Instance dédiée

Un VPC peut avoir une location de default ou dedicated. Par défaut, vos VPC bénéficient d'une location default et vos instances lancées dans un VPC de location default bénéficient d'une location default. Pour lancer des instances dédiées, procédez comme suit :

- Créez un VPC avec une location dedicated, afin que toutes les instances du VPC s'exécutent en tant qu'instances dédiées. Pour plus d'informations, consultez [Créer un VPC avec une location d'instance dédiée](#).

- Créez un VPC avec une location default et spécifiez manuellement une location dedicated pour que les instances s'exécutent en tant qu'instances dédiées. Pour plus d'informations, consultez [Lancer une instances dédiées sur un VPC](#).

Fonctionnalités prises en charge

Les instances dédiées prennent en charge les fonctionnalités et intégrations AWS de services suivantes :

Rubriques

- [Instances réservées](#)
- [Dimensionnement automatique](#)
- [Récupération automatique](#)
- [instances Spot dédiées](#)
- [Instances de performance à capacité extensible](#)

Instances réservées

Pour réserver de la capacité pour vos instances dédiées, vous pouvez acheter des instances réservées dédiées ou des réservations de capacité. Pour plus d'informations, consultez [Reserved instances](#) et [On-Demand Capacity Reservations](#).

Quand vous achetez une Instance réservée dédiée, vous achetez la capacité nécessaire pour lancer une Instance dédiée dans un VPC à un coût d'utilisation grandement réduit ; la rupture de prix sur le coût d'utilisation s'applique uniquement si vous lancez une instance avec une location dédiée. Lorsque vous achetez une Instance réservée avec une location par défaut, celle-ci s'applique uniquement à une instance en cours d'exécution dotée d'un location default. Elle ne s'appliquerait pas à une instance en cours d'exécution dotée d'une location dedicated.

Vous ne pouvez pas utiliser le processus de modification pour modifier la location d'une Instance réservée après l'avoir achetée. Par contre, vous pouvez échanger une Instance réservée convertible contre une nouvelle Instance réservée convertible avec une autre location.

Dimensionnement automatique

Vous pouvez utiliser Amazon EC2 Auto Scaling pour lancer des instances dédiées. Pour plus d'informations, consultez [Lancement d'instances Auto Scaling dans un VPC](#) dans le Amazon EC2 Auto Scaling Guide de l'utilisateur.

Récupération automatique

Vous pouvez configurer la restauration automatique pour une instance dédiée si celle-ci est altérée en raison d'une défaillance matérielle sous-jacente ou d'un problème nécessitant une AWS intervention pour être réparé. Pour plus d'informations, consultez [Résilience de l'instance](#).

instances Spot dédiées

Vous pouvez exécuter une instance Spot dédiée en spécifiant une location `dedicated` lorsque vous créez une demande d'instance Spot. Pour plus d'informations, consultez [Spécifier une location pour votre instances Spot](#).

Instances de performance à capacité extensible

Vous pouvez tirer parti des avantages liés à une exécution sur du matériel à location dédiée avec [the section called "Instance de performance à capacité extensible"](#). Par défaut, les instances dédiées T3 sont lancées en mode illimité. Leur niveau de performances d'UC de base peut être étendu à un niveau supérieur lorsque la charge de travail l'exige. Les performances de base T3 et la possibilité d'émettre en rafale sont régies par les crédits UC. Compte tenu de la nature extensible des types d'instance T3, pour des performances optimales, nous vous recommandons de surveiller la façon dont vos instances T3 utilisent les ressources d'UC du matériel dédié. Les instances dédiées T3 s'adressent à des clients dont les charges de travail variées présentent un comportement d'UC aléatoire, mais dont le niveau d'utilisation d'UC est de préférence moyen ou inférieur aux niveaux d'utilisation de base. Pour plus d'informations, consultez [the section called "Concepts clés"](#).

Amazon EC2 dispose de systèmes qui permettent d'identifier et de corriger les fluctuations au niveau des performances. Cependant, il est toujours possible d'observer des fluctuations à court terme si vous lancez plusieurs instances dédiées T3 dont les modèles d'utilisation de CPU sont corrélés. Pour les charges de travail plus exigeantes ou corrélées, nous recommandons d'utiliser des instances dédiées M5 ou M5 plutôt que des instances dédiées T3.

Limites de instances dédiées

Gardez les points suivants à l'esprit lorsque vous utilisez des instances dédiées :

- Certains AWS services ou leurs fonctionnalités ne sont pas pris en charge par un VPC dont la location d'instance est définie sur `dedicated`. Vérifiez la documentation du service pour confirmer s'il existe des restrictions.

- Certains types d'instance ne peuvent pas être lancés dans un VPC dont la location d'instance est définie comme `dedicated`. Pour plus d'informations sur les types d'instance pris en charge, consultez [Amazon EC2 Dedicated instances](#) (Instance dédiées Amazon EC2).
- Quand vous lancez une Instance dédiée Amazon EBS, le volume EBS ne s'exécute pas sur un matériel dédié à utilisateur unique.

Tarifification des instances dédiées

La tarification des instances dédiées est différente de celle des instances à la demande. Pour plus d'informations, consultez la [page produit des Instances dédiées Amazon EC2](#).

Travailler avec instances dédiées

Vous pouvez créer un VPC avec une location d'instance `dedicated` afin de veiller à ce que toutes les instances lancées dans le VPC soient des Instances dédiées. Vous pouvez aussi spécifier la location de l'instance lors du lancement.

Rubriques

- [Créer un VPC avec une location d'instance dédiée](#)
- [Lancer une instances dédiées sur un VPC](#)
- [Afficher les informations de location](#)
- [Modifier la location d'une instance](#)
- [Modifier la location d'un VPC](#)

Créer un VPC avec une location d'instance dédiée

Quand vous créez un VPC, vous avez la possibilité de spécifier sa location d'instance. Si vous lancez une instance dans un VPC qui a une location d'instance `dedicated`, l'instance sera toujours une instance dédiée sur du matériel qui est dédié à votre usage.

Pour plus d'informations sur la création d'un VPC et le choix des options de location, consultez [Création d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.

Lancer une instances dédiées sur un VPC

Vous pouvez lancer une Instance dédiée à l'aide de l'assistant de lancement d'instance Amazon EC2.

Console

Pour lancer une Instance dédiée dans un VPC de location par défaut à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances, Launch instance (Lancer une instance).
3. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez une AMI de la liste.
4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance à lancer.

Note

Veillez à choisir un type d'instance pris en charge en tant qu'Instance dédiée. Pour plus d'informations, consultez [Instances dédiées Amazon EC2](#).

5. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à associer à l'instance.
6. Dans la section Advanced details, pour Tenancy (Location), sélectionnez Dedicated (Dédié).
7. Configurez les options d'instance restantes selon les besoins. Pour plus d'informations, consultez [Lancer une instance à l'aide de paramètres définis](#).
8. Sélectionnez Launch instance (Lancer une instance).

Command line

Pour définir l'option de location pour une instance lors du lancement à l'aide de la ligne de commande

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (AWS Tools for Windows PowerShell)

Pour plus d'informations sur le lancement d'une instance avec une location host, consultez [Lancer des instances sur un Hôte dédié](#).

Afficher les informations de location

Console

Pour afficher les informations de location pour votre VPC à l'aide de la console

1. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, sélectionnez Vos VPC.
3. Vérifiez la location d'instance de votre VPC dans la colonne Tenancy.
4. Si la colonne Location n'est pas affichée, choisissez settings  dans le coin supérieur droit, activez la location et choisissez Confirmer.

Pour afficher les informations de location pour votre instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Vérifiez la location de votre instance dans la colonne Tenancy.
4. Si la colonne Location n'est pas affichée, effectuez l'une des opérations suivantes :
 - Choisissez paramètres  dans le coin supérieur droit, activez la location et choisissez Confirmer.
 - Sélectionnez l'instance. Sous l'onglet Details (Détails) situé en bas de la page, sous Host and placement group (Hôte et groupe de placement), vérifiez la valeur de Tenancy (Location).

Command line

Pour décrire la location de votre VPC à l'aide de la ligne de commande

- [describe-vpcs](#) (AWS CLI)
- [Get-EC2Vpc](#) (AWS Tools for Windows PowerShell)

Pour décrire la location de votre instance à l'aide de la ligne de commande

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (AWS Tools for Windows PowerShell)

Pour décrire la valeur de location d'une Instance réservée à l'aide de la ligne de commande

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (AWS Tools for Windows PowerShell)

Pour décrire la valeur de location d'une offre d'Instance réservée à l'aide de la ligne de commande

- [describe-reserved-instances-offerings](#) (AWS CLI)
- [Get-EC2ReservedInstancesOffering](#) (AWS Tools for Windows PowerShell)

Modifier la location d'une instance

Vous pouvez modifier la location d'une instance arrêtée après l'avoir lancée. Les modifications que vous apportez prennent effet au prochain démarrage de l'instance.

Les détails du système d'exploitation de votre instance, et le fait que SQL Server soit installé ou non, ont une incidence sur les conversions prises en charge. Pour plus d'informations sur les chemins de conversion de location disponibles pour votre instance, consultez la section [Tenancy conversion](#) dans le Guide de l'utilisateur de License Manager.

Note

Pour les instances T3, vous devez lancer l'instance sur un hôte dédié pour utiliser une location `host`. Vous ne pouvez pas modifier la location de `host` à `dedicated` ou `default`. Si vous tentez d'effectuer l'une de ces modifications de location non prises en charge, vous obtiendrez un code d'erreur `InvalidRequest`.

Console

Pour modifier la location d'une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le volet de navigation, sélectionnez Instances, puis choisissez votre instance.
3. Sélectionnez Instance state (État de l'instance), Stop instance (Arrêter l'instance), Stop (Arrêter).
4. Choisissez Actions, Paramètres de l'instance, puis Modifier le placement d'instance.
5. Pour Tenancy (Location), choisissez d'exécuter votre instance sur un matériel dédié ou sur un Hôte dédié. Choisissez Enregistrer.

Command line

Pour modifier la valeur de location d'une instance à l'aide de la ligne de commande

- [modify-instance-placement](#) (AWS CLI)
- [Edit-EC2InstancePlacement](#) (AWS Tools for Windows PowerShell)

Modifier la location d'un VPC

Vous pouvez modifier la location d'instance d'un VPC en remplaçant `dedicated` par `default` après l'avoir créé. La modification de la location d'instance du VPC n'affecte pas la location des instances figurant dans le VPC. La prochaine fois que vous lancerez une instance dans ce VPC, elle aura une location `default`, à moins que vous ne spécifiez une autre option lors du lancement.

Note

Vous ne pouvez pas modifier la location d'instance d'un VPC en remplaçant `default` par `dedicated` après l'avoir créé.

Vous pouvez modifier la location d'instance d'un VPC à l'aide d'AWS un SDK ou de AWS CLI l'API Amazon EC2 uniquement.

Command line

Pour modifier l'attribut de location d'instance d'un VPC à l'aide du AWS CLI

Utilisez la commande [modify-vpc-tenancy](#) et spécifiez l'ID du VPC et la valeur de location d'instance. La seule valeur prise en charge est `default`.

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

Réserve de capacité

La réserve de capacité à la demande vous permet de réserver de la capacité de calcul pour les instances Amazon EC2 dans une zone de disponibilité spécifique. Il existe deux types de réserve de capacité qui répondent à différents cas d'utilisation.

Types de réserve de capacité

- On-Demand Capacity Reservations
- Blocs de capacité pour ML

Voici quelques cas d'utilisation courants de la réserve de capacité à la demande :

- Événements de mise à l'échelle : créez une réserve de capacité avant les événements stratégiques afin de pouvoir effectuer une mise à l'échelle lorsque vous en avez besoin.
- Exigences réglementaires et reprise après sinistre : utilisez la réservation de capacité à la demande pour satisfaire aux exigences réglementaires en matière de haute disponibilité, et effectuez une réserve de capacité dans une zone de disponibilité ou une région différente pour la reprise après sinistre.

Voici quelques cas d'utilisation courants des blocs de capacité pour ML :

- Entraînement et optimisation du modèle de machine learning (ML) : bénéficiez d'un accès ininterrompu aux instances GPU que vous avez réservées pour terminer l'entraînement et l'optimisation du modèle de machine learning.
- Expérimentations et prototypes de machine learning : exécutez des expériences et créez des prototypes qui nécessitent des instances de GPU pendant de courtes durées.

Quand utiliser la réserve de capacité à la demande

Utilisez la réserve de capacité à la demande si vous avez des exigences de capacité strictes et si vous exécutez des charges de travail critiques qui nécessitent une garantie de capacité. Avec la réserve de capacité à la demande, vous pouvez vous assurer d'avoir toujours accès à la capacité Amazon EC2 que vous avez réservée, pendant aussi longtemps que nécessaire.

Quand utiliser les blocs de capacité pour ML

Utilisez les blocs de capacité pour ML lorsque vous devez vous assurer de disposer d'un accès ininterrompu aux instances GPU pendant une période définie à compter d'une date ultérieure. Les blocs de capacité conviennent parfaitement à l'entraînement et à l'optimisation des modèles de machine learning, aux expérimentations de courte durée et à la gestion des augmentations temporaires de la demande d'inférence à venir. Avec les blocs de capacité, vous pouvez vous assurer d'avoir accès aux ressources GPU à une date spécifique pour exécuter vos charges de travail de machine learning.

On-Demand Capacity Reservations

Réservations de capacité à la demande vous permet de réserver de la capacité de calcul pour vos instances Amazon EC2 dans une zone de disponibilité spécifique pour la durée de votre choix. Les réserves de capacité atténuent le risque de ne pas pouvoir obtenir de capacité à la demande en cas de contraintes en matière de capacité. Si vous avez des exigences strictes en matière de capacité et que vous exécutez des charges de travail stratégiques qui nécessitent un certain niveau de garantie de capacité à long ou à court terme, nous vous recommandons de créer une réserve de capacité afin de vous assurer d'avoir toujours accès à la capacité Amazon EC2 quand vous en avez besoin, aussi longtemps que vous en avez besoin.

Vous pouvez créer des réserves de capacité à tout moment, sans avoir à vous engager pour une durée de 1 à 3 ans. La capacité devient disponible et la facturation démarre dès que la réserve de capacité est allouée dans votre compte. Lorsque vous n'avez plus besoin de la garantie de capacité, annulez la réserve de capacité pour libérer de la capacité et ne plus encourir de frais. Vous pouvez également utiliser les remises de facturation proposées par les Savings Plans et les instances réservées régionales pour réduire le coût d'une réserve de capacité.

Lorsque vous créez un Réservation de capacité, vous spécifiez :

- Zone de disponibilité dans laquelle la capacité est réservée
- Nombre d'instances pour lesquelles vous souhaitez réserver la capacité
- Les attributs de l'instance, y compris le type d'instance, la plate-forme, la zone de disponibilité et la location

Réservations de capacité peut uniquement être utilisé par les instances correspondant aux attributs. Par défaut, elles sont automatiquement utilisées par les instances en cours d'exécution dont les attributs correspondent. Si vous n'avez aucune instance en cours d'exécution dont les attributs correspondent à ceux de la Réservation de capacité, celle-ci reste inutilisée jusqu'à ce que vous lanciez une instance dont les attributs correspondent.

Table des matières

- [Différences entre les réservations de capacité, les instances réservées et les Savings Plans](#)
- [Plateformes prises en charge](#)
- [Quotas](#)
- [Limites](#)
- [Tarification et facturation d'une Réservation de capacité](#)
- [Utiliser réservations de capacité](#)
- [Utiliser des groupes de Réservation de capacité](#)
- [Réserves de capacité dans des groupes de placement de cluster](#)
- [Réservations de capacité dans Local Zones](#)
- [Réservations de capacité dans les zones Wavelength](#)
- [Réservations de capacité sur AWS Outposts](#)
- [Utiliser des réservations de capacité partagées](#)
- [Flottes de réservation de capacité](#)
- [Surveillance des réserves de capacité](#)

Différences entre les réservations de capacité, les instances réservées et les Savings Plans

Le tableau suivant met en évidence les principales différences entre les réservations de capacité, les instances réservées et les Savings Plans :

	Capacity Reservations	instances réservées zonales	instances réservées régionales	Savings Plans
Durée	Aucun engagement requis. Peuvent être créées et annulées selon les besoins.	Exige un engagement d'un an ou de trois ans		
Avantage de capacité	Capacité réservée dans une zone de disponibilité spécifique.	Aucune capacité réservée.		

	Capacity Reservations	instances réservées zonales	instances réservées régionales	Savings Plans
Remise de facturation	Pas de remise de facturation. †	Fournit une remise de facturation.		
Limites d'instance	Vos limites instance à la demande par région s'appliquent.	La valeur par défaut est de 20 par zone de disponibilité. Vous pouvez demander une augmentation de limite.	La valeur par défaut est de 20 par région. Vous pouvez demander une augmentation de limite.	Aucune limite.

† Vous pouvez combiner les réservations de capacité avec des Savings Plans ou des instances réservées régionales pour bénéficier d'une remise.

Pour plus d'informations, consultez les ressources suivantes :

- [Reserved instances](#)
- [Guide de l'utilisateur Savings Plans](#)

Plateformes prises en charge

Vous devez créer la réservation de capacité avec la plateforme appropriée pour vous assurer qu'elle correspond à vos instances. Les réservations de capacité prennent en charge les plateformes suivantes :

- Linux/Unix
- Linux avec SQL Server Standard
- Linux avec SQL Server Web
- Linux avec SQL Server Enterprise
- SUSE Linux

- Utilisation de Red Hat Enterprise Linux
- RHEL avec SQL Server Standard
- RHEL avec SQL Server Enterprise
- RHEL avec SQL Server Web
- RHEL avec HA
- RHEL avec HA et SQL Server Standard
- RHEL avec HA et SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows avec SQL Server
- Windows avec SQL Server Web
- Windows avec SQL Server Standard
- Windows avec SQL Server Enterprise

Lorsque vous achetez une Réserve de capacité, vous devez spécifier la plateforme qui correspond au système d'exploitation de votre instance.

- Pour les distributions SUSE Linux et RHEL, à l'exclusion de BYOL, vous devez choisir la plateforme spécifique. Par exemple, la plateforme SUSE Linux ou Red Hat Enterprise Linux.
- Pour toutes les autres distributions Linux (y compris Ubuntu), choisissez la plateforme Linux/UNIX.
- Si vous apportez votre propre abonnement RHEL (BYOL) actuel, vous devez choisir la plateforme Linux/UNIX.
- Pour Windows avec SQL Standard, Windows avec SQL Server Enterprise et Windows avec SQL Server Web, vous devez choisir la plateforme spécifique.
- Pour toutes les autres versions de Windows, à l'exception de BYOL qui n'est pas pris en charge, choisissez la plateforme Windows.

Quotas

Le nombre d'instances pour lesquelles vous êtes autorisé à réserver de la capacité est basé sur le quota d'instances à la demande de votre compte. Vous pouvez réserver de la capacité pour autant d'instances que ce quota le permet, moins le nombre d'instances que vous exécutez déjà.

Les quotas s'appliquent uniquement aux instances en cours d'exécution. Si votre instance est en attente, en arrêt, arrêtée ou mise en veille prolongée, elle n'est pas prise en compte dans votre quota.

Limites

Avant de créer des réservations de capacité, prenez note des limitations et restrictions suivantes.

- Les réservations de capacité actifs et non utilisés sont pris en compte dans vos limites d'instance à la demande.
- Les réservations de capacité ne sont pas transférables d'un AWS compte à un autre. Toutefois, vous pouvez partager les réservations de capacité avec d'autres AWS comptes. Pour plus d'informations, consultez [Utiliser des réservations de capacité partagées](#).
- Les remises de facturation sur les Instance réservée par zone ne s'appliquent pas aux réservations de capacité.
- Les réserves de capacité ne peuvent pas être créées dans des groupes de placement de cluster. Les groupes de placement par répartition et par partition ne sont pas pris en charge.
- Les réservations de capacité ne peuvent pas être utilisés avec des Hôtes dédiés. Les réserves de capacité peuvent être utilisées avec les instances dédiées.
- [Instances Windows] Les réservations de capacité ne peuvent pas être utilisées avec la licence Bring Your Own (BYOL).
- Les réservations de capacité ne vous assurent pas qu'une instance en veille prolongée peut reprendre après avoir essayé de la démarrer.

Tarifification et facturation d'une Réserve de capacité

Rubriques

- [Tarification](#)
- [Facturation](#)
- [Remises de facturation](#)
- [Affichage d'une facture](#)

Tarifification

Les réserves de capacité sont facturées au tarif à la demande équivalent, que vous exécutiez des instances dans la capacité réservée ou non. Si vous n'utilisez pas la réservation, celle-ci apparaîtra

en tant que réservation non utilisée sur votre facture Amazon EC2. Lorsque vous exécutez une instance qui correspond aux attributs d'une réservation, vous payez seulement pour l'instance, vous ne payez rien pour la réservation. Il n'y a aucun frais anticipé ou additionnel.

Par exemple, si vous créez une Réservation de capacité pour 20 instances Linux `m4.large` et que vous exécutez 15 instances Linux `m4.large` dans la même zone de disponibilité, vous serez facturé pour 15 instances actives et pour 5 instances non utilisées dans la réservation.

Les remises de facturation pour les Savings Plans et les Instances réservées régionales s'appliquent aux Réservations de capacité. Pour plus d'informations, consultez [Remises de facturation](#).

Pour plus d'informations, consultez [Tarification Amazon EC2](#).

Facturation

La facturation commence dès que la réserve de capacité est allouée dans votre compte, et elle se poursuit tant que la réserve de capacité reste allouée dans votre compte.

Les réservations de capacité sont facturées à la seconde. Cela signifie que vous êtes facturé pour les heures partielles. Par exemple, si une réserve de capacité reste active dans votre compte pendant 24 heures et 15 minutes, vous serez facturé pour 24,25 heures de réservation.

L'exemple suivant présente la manière dont une Réservation de capacité est facturée. La Réservation de capacité est créée pour une instance Linux `m4.large`, dont le tarif à la demande est de 0,10 USD par heure d'utilisation. Dans cet exemple, la réserve de capacité est allouée dans le compte pendant cinq heures. La Réservation de capacité n'étant pas utilisée la première heure, elle est facturée en tant qu'heure non utilisée au tarif à la demande standard du type d'instance `m4.large`. De la deuxième à la cinquième heure, la Réservation de capacité est occupée par une instance `m4.large`. Pendant ce laps de temps, la Réservation de capacité n'engendre pas de frais, et le compte est facturé pour l'instance `m4.large` qui l'occupe. Pour la sixième heure, la Réservation de capacité est annulée et l'instance `m4.large` s'exécute normalement en dehors de la capacité réservée. Cette heure est facturée selon le tarif à la demande du type d'instance `m4.large`.

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	\$0.10	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.10
On-demand Instance Usage	\$0.00	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.50
Hourly cost	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10	\$0.60

Remises de facturation

Les remises de facturation pour les Savings Plans et les instances réservées régionales s'appliquent aux réservations de capacité. AWS applique automatiquement ces remises aux réservations de capacité dont les attributs correspondent. Lorsqu'un Réservation de capacité est utilisé par une instance, la remise est appliquée à cette instance. Les remises sont prioritairement appliquées à des instances en cours d'exécution avant de couvrir les réservations de capacité inutilisées.

Les remises de facturation sur les instances réservées zonales ne s'appliquent pas aux réservations de capacité.

Pour plus d'informations, consultez les ressources suivantes :

- [Reserved instances](#)
- [Guide de l'utilisateur Savings Plans](#)
- [Options de facturation et d'achat](#)

Affichage d'une facture

Vous pouvez consulter les frais et les frais associés à votre compte sur la AWS Billing and Cost Management console.

- Le Tableau de bord affiche un récapitulatif des dépenses de votre compte.
- Sur la page Factures, sous Détails, développez la section Elastic Compute Cloud et la région pour obtenir des informations de facturation sur vos Réservations de capacité.

Vous pouvez consulter les frais en ligne ou télécharger un fichier CSV. Pour plus d'informations, consultez [Éléments de ligne de réservation de capacité](#) dans le Guide de l'utilisateur AWS Billing and Cost Management .

Utiliser réservations de capacité

Pour commencer à utiliser des réservations de capacité, vous créez la réservation de capacité dans la zone de disponibilité requise. Vous pouvez ensuite lancer des instances dans la capacité réservée, afficher son utilisation de capacité en temps réel, et augmenter ou diminuer ses capacités en fonction de vos besoins.

Par défaut, les réservations de capacité correspondent automatiquement aux nouvelles instances et aux instances en cours d'exécution dont les attributs correspondent (type d'instance, plateforme,

zone de disponibilité et location). Cela signifie que toute instance avec des attributs correspondants est exécutée automatiquement dans la Réserve de capacité. Cependant, vous pouvez également cibler une Réserve de capacité pour des charges de travail spécifiques. Cela vous permet de contrôler explicitement les instances autorisées à s'exécuter dans cette capacité réservée.

Vous pouvez spécifier comment votre réservation prend fin. Vous pouvez choisir d'annuler la Réserve de capacité ou de la terminer automatiquement à une date et une heure spécifiées. Si vous spécifiez une date et une heure de fin, la Réserve de capacité est annulée dans l'heure du moment spécifié. Par exemple, si vous spécifiez la date du 31/5/2019 à 13:30:55, la Réserve de capacité est assurée de prendre fin le 31/5/2019, entre 13:30:55 et 14:30:55. Lorsque la réservation prend fin, vous ne pouvez plus cibler d'instances sur la Réserve de capacité. Les instances en cours d'exécution dans la capacité réservée continuent à s'exécuter sans interruption. Si des instances ciblant une Réserve de capacité sont arrêtées, vous ne pouvez pas les redémarrer avant de supprimer leur préférence de ciblage de Réserve de capacité ou de les configurer de manière à cibler une Réserve de capacité différente.

Table des matières

- [Créer une Réserve de capacité](#)
- [Lancer des instances dans une Réserve de capacité existante](#)
- [Modifier une Réserve de capacité](#)
- [Modifier les paramètres Réserve de capacité d'une instance](#)
- [Afficher une Réserve de capacité](#)
- [Annuler une Réserve de capacité](#)

Créer une Réserve de capacité

Si votre demande de création d'une réserve de capacité aboutit, la capacité est disponible immédiatement. La capacité demeure réservée pour votre utilisation tant que la Réserve de capacité est active. Vous pouvez y lancer des instances à tout moment. Si la Réserve de capacité est ouverte, les nouvelles instances et les instances existantes dont les attributs correspondent s'exécutent automatiquement dans la capacité de la Réserve de capacité. Si la Réserve de capacité est `targeted`, les instances doivent la cibler spécifiquement pour s'exécuter dans la capacité réservée.

Votre demande de création d'une Réserve de capacité peut échouer si l'une des situations suivantes se produit :

- Amazon EC2 n'a pas une capacité suffisante pour répondre à la demande. Réessayez ultérieurement, essayez une zone de disponibilité différente ou essayez une demande moins importante. Si votre application tolère plusieurs types et tailles d'instance, essayez des attributs d'instance différents.
- La quantité demandée dépasse votre limite d'instance à la demande pour la famille de l'instance sélectionnée. Augmentez votre limite d'instance à la demande pour la famille de l'instance requise et réessayez. Pour plus d'informations, consultez [Quotas des instances à la demande](#).

Pour créer une Réserve de capacité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Réservations de capacité, puis Créer Réserve de capacité.
3. Sur la page Create a Réserve de capacité (Créer une capacité de réservation), configurez les paramètres suivants dans la section Instance details (Détails de l'instance). Le type d'instance, la plateforme, la zone de disponibilité et la location des instances que vous lancez doivent correspondre au type d'instance, à la plateforme, à la zone de disponibilité et à la location que vous spécifiez ici, sinon la réservation de capacité n'est pas appliquée. Par exemple, si un Réserve de capacité ouvert ne correspond pas, un lancement d'instance ciblant ce Réserve de capacité explicitement échouera.
 - a. Type d'instance : type d'instance à lancer dans la capacité réservée.
 - b. Launch EBS-optimized instances (Lancer des instances optimisées pour EBS) : spécifiez si vous souhaitez réserver la capacité pour des instances optimisées pour EBS. Cette option est sélectionnée par défaut pour certains types d'instances. Pour plus d'informations, consultez [the section called "Optimisation EBS"](#).
 - c. Plateforme : système d'exploitation pour vos instances. Pour plus d'informations, consultez [Plateformes prises en charge](#).
 - d. Zone de disponibilité : zone de disponibilité dans laquelle réserver la capacité.
 - e. Emplacement : spécifiez si vous voulez exécuter sur un matériel partagé (par défaut) ou une instance dédiée.
 - f. (Facultatif) Groupe de placement ARN : ARN du groupe de placement du cluster dans lequel créer la réserve de capacité.

Pour plus d'informations, consultez [Réserve de capacité dans des groupes de placement de cluster](#).

La commande suivante crée une réservation de capacité qui réserve de la capacité à trois `m5.2xlarge` instances exécutant Windows avec des AMI SQL Server dans la zone de `us-east-1a` disponibilité.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-  
platform Windows with SQL Server --availability-zone us-east-1a --instance-count 3
```

Lancer des instances dans une Réserve de capacité existante

Lorsque vous lancez une instance, vous pouvez spécifier si elle doit être lancée dans n'importe quel Réserve de capacité open, dans une Réserve de capacité spécifique, ou dans un groupe de Réservations de capacité. Vous ne pouvez lancer une instance que dans le cadre d'une réservation de capacité qui possède les attributs correspondants (type d'instance, plateforme, zone de disponibilité et location) et une capacité suffisante. Vous pouvez également configurer l'instance pour éviter qu'elle s'exécute dans une Réserve de capacité, même si vous avez une Réserve de capacité open qui a des attributs correspondants et la capacité disponible.

Le lancement d'une instance dans une Réserve de capacité réduit sa capacité disponible du nombre d'instances lancées. Par exemple, si vous lancez trois instances, la capacité disponible de la Réserve de capacité est réduite de trois.

Pour lancer des instances dans une Réserve de capacité existante à l'aide de la console

1. Suivez la procédure pour [lancer une instance](#), mais ne lancez pas l'instance tant que vous n'avez pas effectué les étapes suivantes pour spécifier les paramètres du groupe de placement et de la réservation de capacité.
2. Développez les informations avancées et procédez comme suit :
 - a. Pour Groupe de placement, sélectionnez le groupe de placement du cluster dans lequel vous souhaitez lancer l'instance.
 - b. Pour Capacity Reservation (Réserve de capacité), choisissez l'une des options suivantes en fonction de la configuration de la réserve de capacité :
 - Aucune — Empêche les instances de se lancer dans une réservation de capacité. Les instances s'exécutent dans une capacité à la demande.
 - Ouvert — Lance les instances dans n'importe quelle réservation de capacité dont les attributs correspondent et une capacité suffisante pour le nombre d'instances que vous avez sélectionné. Si vous n'avez pas de Réserve de capacité correspondante avec une capacité suffisante, l'instance utilise une capacité à la demande.

- Cibler par ID — Lance les instances dans la réservation de capacité sélectionnée. Si la Réserve de capacité sélectionnée ne dispose pas d'une capacité suffisante pour le nombre d'instances que vous avez sélectionnées, le lancement de l'instance échoue.
 - Cibler par groupe : lance les instances dans n'importe quelle réservation de capacité avec les attributs correspondants et la capacité disponible dans le groupe de réservation de capacité sélectionné. Si le groupe sélectionné ne dispose pas d'une Réserve de capacité avec les attributs correspondants et de la capacité disponible, les instances s'exécutent à l'aide de la capacité à la demande.
3. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Pour lancer une instance dans une réservation de capacité existante à l'aide du AWS CLI

Utilisez la commande [run-instances](#) et spécifiez le paramètre `--capacity-reservation-specification`.

L'exemple suivant lance une instance `t2.micro` dans toute Réserve de capacité ouverte disposant des attributs correspondants et de la capacité disponible :

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
--key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationPreference=open
```

L'exemple suivant lance une instance `t2.micro` dans un targeted Réserve de capacité :

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
--key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

L'exemple suivant lance une instance `t2.micro` dans un groupe Réserve de capacité :

```
aws ec2 run-instances --image-id ami-abc12345 --count 1
--instance-type t2.micro --key-name MyKeyPair --subnet-
id subnet-1234567890abcdef1 --capacity-reservation-specification
CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Modifier une Réserve de capacité

Vous pouvez modifier les attributs d'une Réserve de capacité active après l'avoir créée. Vous ne pouvez pas modifier une Réserve de capacité après son expiration ou après l'avoir explicitement annulée.

Lors de la modification d'une Réserve de capacité, vous pouvez uniquement augmenter ou diminuer la quantité et modifier la manière dont elle est libérée. Vous ne pouvez pas modifier le type d'instance, l'optimisation EBS, la plateforme, la zone de disponibilité ou l'éligibilité d'instance d'une Réserve de capacité. Si vous devez modifier un de ces attributs, nous vous recommandons d'annuler la réservation, puis d'en créer une nouvelle avec les attributs requis.

Si vous spécifiez une nouvelle quantité qui dépasse votre limite d'instance à la demande restante pour le type d'instance sélectionné, la mise à jour échoue.

Pour modifier une Réserve de capacité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Réservations de capacité, sélectionnez la Réserve de capacité à modifier, puis choisissez Modifier.
3. Modifiez les options Quantité ou Reservation ends (Fins de réservation) selon vos besoins, puis choisissez Enregistrer les modifications.

Pour modifier une réservation de capacité à l'aide du AWS CLI

Utilisez la commande [modify-capacity-reservation](#) :

Par exemple, la commande suivante modifie une Réserve de capacité pour réserver la capacité pour huit instances.

```
aws ec2 modify-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0 --  
instance-count 8
```

Modifier les paramètres Réserve de capacité d'une instance

Vous pouvez modifier les paramètres de Réserve de capacité pour une instance arrêtée à tout moment :

- Commencez par n'importe quelle réservation de capacité dont les attributs (type d'instance, plateforme, zone de disponibilité et location) et la capacité disponible correspondent.

- Démarrez l'instance dans une Réserve de capacité spécifique.
- Démarrez dans n'importe quelle Réserve de capacité qui dispose des attributs correspondants et de la capacité disponible dans un groupe Réserve de capacité
- Empêchez l'instance de démarrer dans une Réserve de capacité.

Pour modifier les paramètres de la Réserve de capacité d'une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Instances, puis sélectionnez l'instance à modifier. Arrêtez l'instance, si elle ne l'est pas déjà.
3. Choisissez Actions, Paramètres de l'instance, Modifier les paramètres de réservation de capacité.
4. Pour Réserve de capacité, choisissez l'une des options suivantes :
 - Open (Ouvrir) : lance les instances dans toute Réserve de capacité comportant des attributs correspondants et une capacité suffisante pour le nombre d'instances que vous avez sélectionnées. Si vous n'avez pas de Réserve de capacité correspondante avec une capacité suffisante, l'instance utilise une capacité à la demande.
 - None (Aucune) : empêche les instances de se lancer dans une Réserve de capacité. Les instances s'exécutent dans une capacité à la demande.
 - Spécifier la réservation de capacité — Lance les instances dans la Réserve de capacité sélectionnée. Si la Réserve de capacité sélectionnée ne dispose pas d'une capacité suffisante pour le nombre d'instances que vous avez sélectionnées, le lancement de l'instance échoue.
 - Spécifier le groupe de réservation de capacité — Lance les instances dans n'importe quelle Réserve de capacité avec les attributs correspondants et la capacité disponible dans le groupe Réserve de capacité sélectionné. Si le groupe sélectionné ne dispose pas d'une Réserve de capacité avec les attributs correspondants et de la capacité disponible, les instances s'exécutent à l'aide de la capacité à la demande.

Pour modifier les paramètres de réservation de capacité d'une instance à l'aide du AWS CLI

Utilisez la commande [modify-instance-capacity-reservation-attributes](#).

Par exemple, la commande suivante change le paramètre Réserve de capacité d'une instance pour open ou none.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-id i-1234567890abcdef0 --capacity-reservation-specification CapacityReservationPreference=none|open
```

Par exemple, la commande suivante modifie une instance pour cibler une Réserve de capacité spécifique.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-id i-1234567890abcdef0 --capacity-reservation-specification CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

Par exemple, la commande suivante modifie une instance pour cibler un groupe Réserve de capacité spécifique.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-id i-1234567890abcdef0 --capacity-reservation-specification CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-groups:us-west-1:123456789012:group/my-cr-group}
```

Afficher une Réserve de capacité

Réservations de capacité peut avoir les états suivants :

- **active** : la capacité peut être utilisée.
- **expired** : la Réserve de capacité a expiré automatiquement à la date et à l'heure spécifiées dans votre demande de réservation. La capacité réservée n'est plus disponible pour utilisation.
- **cancelled** : la Réserve de capacité a été annulée. La capacité réservée n'est plus disponible pour utilisation.
- **pending** : la demande de Réserve de capacité a abouti, mais la mise en service de la capacité est toujours en attente.
- **failed** : la demande de Réserve de capacité a échoué. Une demande peut échouer en raison de paramètres de demande qui ne sont pas valides, de contraintes de capacité ou de contraintes de limite d'instance. Vous pouvez afficher une demande qui a échoué pendant 60 minutes.

Note

En raison du modèle de [cohérence à terme](#) suivi par les API Amazon EC2, une fois la réserve de capacité créée, il peut s'écouler jusqu'à 5 minutes avant que la console et la réponse

[describe-capacity-reservations](#) n'indiquent que la réserve de capacité est dans l'état active. Pendant ce temps, la console et la réponse `describe-capacity-reservations` peuvent indiquer que la réserve de capacité se trouve dans l'état pending. Toutefois, la réserve de capacité peut déjà être utilisée et vous pouvez tenter d'y lancer des instances.

Pour afficher vos réservations de capacité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Réservations de capacité puis sélectionnez une Réserve de capacité à afficher.
3. Choisissez View launched instances for this reservation (Afficher les instances lancées pour cette réservation).

Pour consulter vos réservations de capacité à l'aide du AWS CLI

Utilisez la commande [describe-capacity-reservations](#) :

Par exemple, la commande suivante décrit toutes les réservations de capacité.

```
aws ec2 describe-capacity-reservations
```

Exemple de sortie.

```
{
  "CapacityReservations": [
    {
      "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
      "EndDateType": "unlimited",
      "AvailabilityZone": "eu-west-1a",
      "InstanceMatchCriteria": "open",
      "Tags": [],
      "EphemeralStorage": false,
      "CreateDate": "2019-08-16T09:03:18.000Z",
      "AvailableInstanceCount": 1,
      "InstancePlatform": "Linux/UNIX",
      "TotalInstanceCount": 1,
      "State": "active",
      "Tenancy": "default",
      "EbsOptimized": true,
      "InstanceType": "a1.medium",
    }
  ]
}
```

```
    "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-group/
MyPG"
  },
  {
    "CapacityReservationId": "cr-abcdEXAMPLE9876ef ",
    "EndDateType": "unlimited",
    "AvailabilityZone": "eu-west-1a",
    "InstanceMatchCriteria": "open",
    "Tags": [],
    "EphemeralStorage": false,
    "CreateDate": "2019-08-07T11:34:19.000Z",
    "AvailableInstanceCount": 3,
    "InstancePlatform": "Linux/UNIX",
    "TotalInstanceCount": 3,
    "State": "cancelled",
    "Tenancy": "default",
    "EbsOptimized": true,
    "InstanceType": "m5.large"
  }
]
}
```

Annuler une Réserve de capacité

Vous pouvez annuler une Réserve de capacité à tout moment si vous n'avez plus besoin de la capacité réservée. Lorsque vous annulez une Réserve de capacité, la capacité est immédiatement libérée et n'est plus réservée pour votre utilisation.

Vous pouvez annuler des réservations de capacité vides et des réservations de capacité ayant des instances en cours d'exécution. Si vous annulez une Réserve de capacité avec des instances en cours d'exécution, les instances continuent leur exécution normale en dehors de la réservation de capacité aux tarifs standard instance à la demande ou à un tarif réduit si vous avez un Savings Plans ou une Instance réservée régionale correspondant.

Une fois que vous avez annulé une Réserve de capacité, les instances la ciblant ne peuvent plus être lancées. Modifiez ces instances de sorte qu'elles ciblent une autre Réserve de capacité, lancez-les dans une Réserve de capacité « open » disposant des attributs correspondants et d'une capacité suffisante ou évitez de les lancer dans une Réserve de capacité. Pour plus d'informations, consultez [Modifier les paramètres Réserve de capacité d'une instance](#).

Pour annuler une Réserve de capacité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Réservations de capacité et sélectionnez la Réserve de capacité à annuler.
3. Choisissez Cancel réservation (Annuler la réservation), Cancel réservation (Annuler la réservation).

Pour annuler une réservation de capacité à l'aide du AWS CLI

Utilisez la commande [cancel-capacity-reservation](#) :

Par exemple, la commande suivante annule une Réserve de capacité avec un ID de `cr-1234567890abcdef0`.

```
aws ec2 cancel-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0
```

Utiliser des groupes de Réserve de capacité

Vous pouvez utiliser AWS Resource Groups pour créer des ensembles logiques de réservations de capacité, appelés groupes de ressources. Un groupe de ressources est un regroupement logique de AWS ressources qui se trouvent toutes dans la même AWS région. Pour plus d'informations sur les groupes de ressources, consultez [Que sont les groupes de ressources ?](#) dans le Guide de l'utilisateur AWS Resource Groups .

Vous pouvez inclure les réservations de capacité que vous possédez dans votre compte et les réservations de capacité partagées avec vous par d'autres AWS comptes dans un seul groupe de ressources. Vous pouvez également inclure des réservations de capacité ayant différents attributs (type d'instance, plate-forme, zone de disponibilité et location) dans un seul groupe de ressources.

Lorsque vous créez des groupes de ressources pour des réserves de capacité, vous pouvez cibler des instances vers un groupe de réserves de capacité au lieu d'une réserve de capacité seule. Les instances qui ciblent un groupe de réservations de capacité correspondent à toutes les réservations de capacité du groupe dont les attributs (type d'instance, plate-forme, zone de disponibilité et location) et la capacité disponible correspondent. Si le groupe ne dispose pas d'une Réserve de capacité avec les attributs correspondants et de la capacité disponible, les instances s'exécutent à l'aide de la capacité à la demande. Si une Réserve de capacité adéquate est ajoutée au groupe cible à un stade ultérieur, l'instance est automatiquement mise en correspondance et déplacée vers sa capacité réservée.

Pour empêcher une utilisation non prévue des réservations de capacité dans un groupe, configurez la réservations de capacité dans le groupe pour accepter uniquement les instances qui ciblent explicitement la réserve de capacité. Pour ce faire, définissez l'éligibilité de l'instance sur ciblées (ancienne console) ou Uniquement des instances qui spécifient cette réservation (nouvelle console) lors de la création de la Réserve de capacité à l'aide de la console Amazon EC2. Lorsque vous utilisez le AWS CLI, spécifiez-le `--instance-match-criteria targeted` lors de la création de la réservation de capacité. On s'assure ainsi que seules les instances qui ciblent explicitement le groupe, ou une Réserve de capacité dans le groupe, peuvent s'exécuter dans le groupe.

Si une Réserve de capacité dans un groupe est annulée ou expire alors qu'elle a des instances en cours d'exécution, des dernières sont automatiquement déplacées vers une autre Réserve de capacité dans le groupe qui a des attributs correspondants et la capacité disponible. S'il ne reste pas de réservations de capacité dans le groupe avec les attributs et la capacité disponible correspondants, les instances s'exécutent à l'aide de la capacité à la demande. Si une Réserve de capacité adéquate est ajoutée au groupe cible à un stade ultérieur, l'instance est automatiquement déplacée dans sa capacité réservée.

Rubriques

- [Création d'un groupe de réserves de capacité](#)
- [Ajout d'une réserve de capacité à un groupe](#)
- [Afficher les réserves de capacité dans un groupe](#)
- [Afficher les groupes auxquels appartient une réserve de capacité](#)
- [Suppression d'une réserve de capacité d'un groupe](#)
- [Suppression d'un groupe de réserves de capacité](#)

Création d'un groupe de réserves de capacité

Pour créer un groupe de réserves de capacité

Utilisez la commande [create-group](#) AWS CLI . Pour name, indiquez un nom descriptif pour le groupe et pour configuration, spécifiez deux paramètres de Type demande :

- `AWS::EC2::CapacityReservationPool` pour s'assurer que le groupe de ressources peut être ciblé pour les lancements d'instances
- `AWS::ResourceGroups::Generic` avec `allowed-resource-types` définie sur `AWS::EC2::CapacityReservation` pour s'assurer que le groupe de ressources accepte uniquement les réserves de capacité

Par exemple, la commande suivante crée un groupe nommé MyCRGroup.

```
aws resource-groups create-group --name MyCRGroup --configuration
'{"Type":"AWS::EC2::CapacityReservationPool"}'
'{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Voici un exemple de sortie.

```
{
  "GroupConfiguration": {
    "Status": "UPDATE_COMPLETE",
    "Configuration": [
      {
        "Type": "AWS::EC2::CapacityReservationPool"
      },
      {
        "Type": "AWS::ResourceGroups::Generic",
        "Parameters": [
          {
            "Values": [
              "AWS::EC2::CapacityReservation"
            ],
            "Name": "allowed-resource-types"
          }
        ]
      }
    ]
  },
  "Group": {
    "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
    "Name": "MyCRGroup"
  }
}
```

Ajout d'une réserve de capacité à un groupe

Si vous ajoutez une réserve de capacité qui est partagée avec vous à un groupe et que le partage est annulé, la réserve est automatiquement supprimée du groupe.

Pour ajouter une Réserve de capacité à un groupe

Utilisez la commande AWS CLI [group-resources](#). Pour `group`, spécifiez le nom du groupe auquel ajouter les Réservations de capacité, et pour `resources`, spécifiez les ARN des Réservations de capacité à ajouter. Pour ajouter plusieurs réservations de capacité, séparez les ARN par un espace. Pour obtenir les ARN des réservations de capacité à ajouter, utilisez la AWS CLI commande [describe-capacity-reservations-et-spécifiez-les-identifiants-des-réservations](#) de capacité.

Par exemple, la commande suivante ajoute deux Réservations de capacité à un groupe nommé `MyCRGroup`.

```
aws resource-groups group-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Voici un exemple de sortie.

```
{
  "Failed": [],
  "Succeeded": [
    "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
    "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
  ]
}
```

Afficher les réserves de capacité dans un groupe

Pour afficher les réservations de capacité dans un groupe spécifique

Utilisez la commande [list-group-resources](#) AWS CLI . Pour `group`, spécifiez le nom du groupe.

Par exemple, la commande suivante répertorie les Réservations de capacité dans un groupe nommé `MyCRGroup`.

```
aws resource-groups list-group-resources --group MyCRGroup
```

Voici un exemple de sortie.

```
{
  "QueryErrors": [],
  "ResourceIdentifiers": [
    {
      "ResourceType": "AWS::EC2::CapacityReservation",

```

```
        "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
    },
    {
        "ResourceType": "AWS::EC2::CapacityReservation",
        "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
    }
]
}
```

Note

Le résultat de la commande comprend des réserves de capacité qui vous appartiennent et des réserves de capacité qui sont partagées avec vous.

Afficher les groupes auxquels appartient une réserve de capacité

AWS CLI

Pour afficher les groupes auxquels une réserve de capacité spécifique a été ajoutée

Utilisez la commande d' AWS CLI [get-groups-for-capacity-reservation](#).

Par exemple, la commande suivante répertorie les groupes auxquels une Réserve de capacité `cr-1234567890abcdef1` a été ajoutée.

```
aws ec2 get-groups-for-capacity-reservation --capacity-reservation-
id cr-1234567890abcdef1
```

Voici un exemple de sortie.

```
{
  "CapacityReservationGroups": [
    {
      "OwnerId": "123456789012",
      "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/
MyCRGroup"
    }
  ]
}
```

Note

Si vous spécifiez une réserve de capacité partagée avec vous, la commande renvoie uniquement les groupes de réserves de capacité qui vous appartiennent.

Amazon EC2 console

Pour afficher les groupes auxquels une réserve de capacité spécifique a été ajoutée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation Réservations de capacité, choisissez la Réserve de capacité à afficher, puis Afficher.

Les groupes auxquels la Réserve de capacité a été ajoutée sont répertoriés dans la fiche Groupes.

Note

Si vous choisissez une réserve de capacité partagée avec vous, la console affiche uniquement les groupes de réserves de capacité qui vous appartiennent.

Suppression d'une réserve de capacité d'un groupe

Pour supprimer une Réserve de capacité d'un groupe

Utilisez la commande [ungroup-resources](#) AWS CLI . Pour `group`, spécifiez l'ARN du groupe duquel supprimer la Réserve de capacité, et pour `resources` spécifier les ARN des Réservations de capacité à supprimer. Pour supprimer plusieurs réservations de capacité, séparez les ARN par un espace.

L'exemple suivant montre comment supprimer deux Réservations de capacité d'un groupe nommé MyCRGroup.

```
aws resource-groups ungroup-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Voici un exemple de sortie.

```
{
  "Failed": [],
  "Succeeded": [
    "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd",
    "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
  ]
}
```

Suppression d'un groupe de réserves de capacité

Pour supprimer un groupe

Utilisez la commande [delete-group](#) AWS CLI . Pour group fournissez le nom du groupe à supprimer.

Par exemple, la commande suivante supprime un groupe appelé MyCRGroup.

```
aws resource-groups delete-group --group MyCRGroup
```

Voici un exemple de sortie.

```
{
  "Group": {
    "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
    "Name": "MyCRGroup"
  }
}
```

Réserves de capacité dans des groupes de placement de cluster

Vous pouvez créer des réserves de capacité dans un groupe de placement du cluster afin de réserver la capacité de calcul Amazon EC2 pour vos charges de travail. Les groupes de placement du cluster offrent l'avantage d'une faible latence réseau et d'un débit réseau élevé.

La création d'une réserve de capacité dans un groupe de placement du cluster garantit que vous avez accès à la capacité de calcul dans vos groupes de placement du cluster lorsque vous en avez besoin, aussi longtemps que nécessaire. Ceci est idéal pour réserver la capacité des charges de travail haute performance (HPC) nécessitant une mise à l'échelle du calcul. Vous pouvez réduire votre cluster tout en veillant à ce que la capacité reste disponible pour votre utilisation afin que vous puissiez la remettre à l'échelle en cas de besoin.

Rubriques

- [Limites](#)
- [Utiliser les réserves de capacité dans des groupes de placement de cluster](#)

Limites

Gardez les éléments suivants à l'esprit lorsque vous créez des réserves de capacité dans des groupes de placement du cluster :

- Si une réservation de capacité existante ne se trouve pas dans un groupe de placement, vous ne pouvez pas modifier la réservation de capacité pour réserver de la capacité dans un groupe de placement. Pour réserver une capacité dans un groupe de placement, vous devez créer la réserve de capacité dans le groupe de placement.
- Une fois que vous avez créé une réserve de capacité dans un groupe de placement, vous ne pouvez pas la modifier pour réserver la capacité en dehors du groupe de placement.
- Vous pouvez augmenter votre capacité réservée dans un groupe de placement en modifiant une réserve de capacité existante dans le groupe de placement ou en créant des réserves de capacité supplémentaires dans le groupe de placement. Toutefois, vous augmentez vos chances d'obtenir une erreur de capacité insuffisante.
- Vous ne pouvez pas partager de réserves de capacité qui ont été créées dans un groupe de placement du cluster.
- Vous ne pouvez pas supprimer un groupe de placement du cluster qui a des réserves de capacité active. Vous devez annuler toutes les réserves de capacité du groupe de placement du cluster avant de pouvoir les supprimer.

Utiliser les réserves de capacité dans des groupes de placement de cluster

Pour commencer à utiliser les réserves de capacité avec des groupes de placement de cluster, effectuez les opérations suivantes.

Note

Si vous souhaitez créer une réserve de capacité dans un groupe de placement de cluster existant, ignorez l'étape 1. Ensuite, pour les étapes 2 et 3, spécifiez l'ARN du groupe de placement du cluster existant. Pour plus d'informations sur la manière de trouver l'ARN de

vos groupe de placement de clusters existant, consultez [Afficher les informations sur le groupe de placement](#).

Rubriques

- [Étape 1 : \(Conditionnelle\) Créer un groupe de placement du cluster pour l'utiliser avec une réserve de capacité](#)
- [Étape 2 : Créer une réserve de capacité dans un groupe de placement du cluster](#)
- [Étape 3 : Lancer des instances dans un groupe de placement du cluster](#)

Étape 1 : (Conditionnelle) Créer un groupe de placement du cluster pour l'utiliser avec une réserve de capacité

Effectuez cette étape uniquement si vous devez créer un groupe de placement du cluster. Pour utiliser un groupe de placement du cluster existant, ignorez cette étape, puis pour les étapes 2 et 3, utilisez l'ARN de ce groupe de placement du cluster. Pour plus d'informations sur la manière de trouver l'ARN de votre groupe de placement de clusters existant, consultez [Afficher les informations sur le groupe de placement](#).

Vous pouvez créer le groupe de placement du cluster en employant l'une des méthodes suivantes.

Console

Pour créer un groupe de placement du cluster à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Placement Groups Groupes de placement, puis Create placement group (Créer un groupe de placement).
3. Pour Name (Nom), spécifiez un nom descriptif pour le groupe de placement.
4. Pour Placement strategy (Stratégie de placement), choisissez Cluster.
5. Choisissez Créer un groupe.
6. Dans le tableau des groupes de placement, dans la colonne ARN du groupe, notez l'ARN du groupe de placement de clusters que vous avez créé. Vous en aurez besoin pour la prochaine étape.

AWS CLI

Pour créer un groupe de placement de clusters à l'aide du AWS CLI

Utilisez la commande [create-placement-group](#). Pour `--group-name`, spécifiez un nom descriptif pour le groupe de placement et pour `--strategy`, spécifiez `cluster`.

L'exemple suivant crée un groupe de placement nommé MyPG qui utilise la stratégie de placement `cluster`.

```
aws ec2 create-placement-group \  
  --group-name MyPG \  
  --strategy cluster
```

Notez l'ARN du groupe de placement renvoyé dans la sortie de la commande, car vous en aurez besoin lors de la prochaine étape.

Étape 2 : Créer une réserve de capacité dans un groupe de placement du cluster

Vous créez une réserve de capacité dans un groupe de placement du cluster de la même manière que vous créez n'importe quelle réserve de capacité. Toutefois, vous devez également spécifier l'ARN du groupe de placement du cluster dans lequel créer la réserve de capacité. Pour plus d'informations, consultez [Créer une Réserve de capacité](#).

Considérations

- Le groupe de placement du cluster spécifié doit être en état `available`. Si le groupe de placement du cluster se trouve en état `pending`, `deleting` ou `deleted`, la demande échoue.
- La réserve de capacité et le groupe de placement du cluster doivent se trouver dans la même zone de disponibilité. Si la demande de création de la réserve de capacité spécifie une zone de disponibilité différente de celle du groupe de placement du cluster, la demande échoue.
- Vous pouvez créer des réserves de capacité uniquement pour les types d'instance pris en charge par les groupes de placement du cluster. Si vous spécifiez un type d'instance non pris en charge, la demande échoue. Pour plus d'informations, consultez [Règles et restrictions des groupes de placement du cluster](#).
- Si vous créez une réserve de capacité `open` dans un groupe de placement du cluster et qu'il existe des instances en cours d'exécution possédant des attributs correspondants (ARN du groupe de placement, type d'instance, zone de disponibilité, plateforme et location), ces instances s'exécutent automatiquement dans la réserve de capacité.

- Votre demande de création d'une Réserve de capacité peut échouer si l'une des situations suivantes se produit :
 - Amazon EC2 n'a pas une capacité suffisante pour répondre à la demande. Réessayez ultérieurement, essayez une zone de disponibilité différente ou essayez une capacité moins importante. Si votre charge de travail tolère plusieurs types et tailles d'instance, essayez des attributs d'instance différents.
 - La quantité demandée dépasse votre limite d'instance à la demande pour la famille de l'instance sélectionnée. Augmentez votre limite d'instance à la demande pour la famille de l'instance requise et réessayez. Pour plus d'informations, consultez [Quotas des instances à la demande](#).

Vous pouvez créer la réserve de capacité dans le groupe de placement du cluster en employant l'une des méthodes suivantes.

Console

Pour créer une Réserve de capacité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Réserves de capacité, puis Créer Réserve de capacité.
3. Sur la page Créer une réservation de capacité, spécifiez le type d'instance, la plate-forme, la zone de disponibilité, la location, la quantité et la date de fin selon les besoins.
4. Pour le groupe de placement, sélectionnez l'ARN du groupe de placement du cluster dans lequel vous souhaitez créer la réservation de capacité.
5. Choisissez Créer.

Pour plus d'informations, consultez [Créer une Réserve de capacité](#).

AWS CLI

Pour créer une réservation de capacité à l'aide du AWS CLI

Utilisez la commande [create-capacity-reservation](#). Pour `--placement-group-arn`, spécifiez l'ARN du groupe de placement du cluster dans lequel créer la réserve de capacité.

```
$ aws ec2 create-capacity-reservation \  
  --instance-type instance_type \  
  --instance-platform platform \  
  --availability-zone az \  
  --placement-group-arn arn \  
  --quantity quantity \  
  --end-date end-date \  
  --tags tags \  
  --dry-run
```

```
--instance-count quantity \  
--placement-group-arn placement_group_ARN
```

Pour plus d'informations, consultez [Créer une Réserve de capacité](#).

Étape 3 : Lancer des instances dans un groupe de placement du cluster

Vous lancez une instance dans une réserve de capacité dans un groupe de placement de cluster de la même manière que vous lancez une instance dans n'importe quelle réserve de capacité. Toutefois, vous devez également spécifier l'ARN du groupe de placement du cluster dans lequel lancer l'instance. Pour plus d'informations, consultez [Créer une Réserve de capacité](#).

Considérations

- Si la réserve de capacité est open, vous n'avez pas besoin de spécifier la réserve de capacité dans la demande de lancement de l'instance. Si l'instance possède des attributs (ARN du groupe de placement, type d'instance, zone de disponibilité, plateforme et location) qui correspondent à une réserve de capacité du groupe de placement spécifié, l'instance s'exécute automatiquement dans la réserve de capacité.
- Si la réserve de capacité accepte uniquement les lancements d'instances ciblées, vous devez spécifier la réserve de capacité cible en plus du groupe de placement du cluster dans la demande.
- Si la réserve de capacité fait partie d'un groupe de réserve de capacité, vous devez spécifier le groupe de réserve de capacité cible en plus du groupe de placement du cluster dans la demande. Pour plus d'informations, consultez [Utiliser des groupes de Réserve de capacité](#).

Vous pouvez lancer une instance dans une réserve de capacité d'un groupe de placement du cluster en employant l'une des méthodes suivantes.

Console

Pour lancer des instances dans une Réserve de capacité existante à l'aide de la console

1. Suivez la procédure pour [lancer une instance](#), mais ne lancez pas l'instance tant que vous n'avez pas effectué les étapes suivantes pour spécifier les paramètres du groupe de placement et de la réservation de capacité.
2. Développez les informations avancées et procédez comme suit :

- a. Pour Groupe de placement, sélectionnez le groupe de placement du cluster dans lequel vous souhaitez lancer l'instance.
- b. Pour Capacity Reservation (Réserve de capacité), choisissez l'une des options suivantes en fonction de la configuration de la réserve de capacité :
 - Ouvert : pour lancer les instances dans n'importe quelle réservation de open capacité du groupe de placement du cluster qui possède les attributs correspondants et une capacité suffisante.
 - Cibler par ID : pour lancer les instances dans une réservation de capacité qui n'accepte que les lancements d'instances ciblés.
 - Cibler par groupe — Pour lancer les instances dans n'importe quelle réservation de capacité avec les attributs correspondants et la capacité disponible dans le groupe de réservation de capacité sélectionné.
3. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Pour plus d'informations, consultez [Lancer des instances dans une Réserve de capacité existante](#).

AWS CLI

Pour lancer des instances dans une réservation de capacité existante à l'aide du AWS CLI

Utilisez la commande [run-instances](#). Si vous devez cibler une réserve de capacité spécifique ou un groupe réserve de capacité spécifique, spécifiez le paramètre `--capacity-reservation-specification`. Pour `--placement`, spécifiez le paramètre `GroupName`, puis indiquez le nom du groupe de placement que vous avez créé lors des étapes précédentes.

La commande suivante lance une instance dans une réserve de capacité `targeted` d'un groupe de placement du cluster.

```
$ aws ec2 run-instances \  
  --image-id ami_id \  
  --count quantity \  
  --instance-type instance_type \  
  --key-name key_pair_name \  
  --subnet-id subnetid \  
  --placement placement_group_name
```

```
--capacity-reservation-specification  
CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \  
--placement "GroupName=cluster_placement_group_name"
```

Pour plus d'informations, consultez [Lancer des instances dans une Réserve de capacité existante](#).

Réservations de capacité dans Local Zones

Une zone locale est une extension d'une AWS région géographiquement proche de vos utilisateurs. Ainsi, les ressources créées dans une zone locale peuvent servir les utilisateurs locaux avec des communications à très faible latence. Pour plus d'informations, consultez [Local Zones AWS](#).

Vous pouvez étendre un VPC de sa AWS région parent à une zone locale en créant un nouveau sous-réseau dans cette zone locale. Lorsque vous créez un sous-réseau dans une zone locale, votre VPC est étendu à cette zone locale. Le sous-réseau de la zone locale fonctionne de la même manière que les autres sous-réseaux de votre VPC.

En utilisant des Local Zones, vous pouvez placer des réservations de capacité dans plusieurs emplacements qui sont plus proches de vos utilisateurs. Vous créez et utilisez des réservations de capacité dans Local Zones de la même manière que vous créez et utilisez des réservations de capacité dans les zones de disponibilité standard. Les fonctionnalités et le comportement de correspondance d'instance sont les mêmes. Pour plus d'informations sur les modèles de tarification pris en charge dans les zones locales, consultez les [questions fréquentes \(FAQ\) sur les AWS Local Zones](#).

Considérations

Vous ne pouvez pas utiliser de groupes de réservation de capacité dans une zone locale.

Pour utiliser une réservation de capacité dans une zone locale

1. Activez la zone locale pour l'utiliser dans votre AWS compte. Pour plus d'informations, consultez [S'inscrire à Local Zones](#).
2. Créez une réservation de capacité dans la zone locale. Pour Zone de disponibilité, sélectionnez la zone locale. La zone locale est représentée par un code de AWS région suivi d'un identifiant indiquant l'emplacement, par exemple `us-west-2-lax-1a`. Pour plus d'informations, consultez [Créer une Réserve de capacité](#).

3. Créez un sous-réseau dans la zone locale. Pour Zone de disponibilité, sélectionnez la zone locale. Pour plus d'informations, consultez [Créer un sous-réseau dans votre VPC](#) dans le Guide de l'utilisateur Amazon VPC.
4. Lancez une instance. Pour Sous-réseau, sélectionnez le sous-réseau dans la zone locale (par exemple, subnet-123abc | us-west-2-1ax-1a) et, pour Réserve de capacité, sélectionnez la spécification (open ou ciblez-la par ID) requise pour la réserve de capacité que vous avez créée dans la zone locale. Pour plus d'informations, consultez [Lancer des instances dans une Réserve de capacité existante](#).

Réserve de capacité dans les zones Wavelength

AWS Wavelength permet aux développeurs de créer des applications qui offrent des latences ultra-faibles aux appareils mobiles et aux utilisateurs finaux. Wavelength déploie des services de calcul et de stockage AWS standard à la périphérie des réseaux 5G des opérateurs de télécommunications. Vous pouvez étendre un Amazon Virtual Private Cloud (VPC) à une ou plusieurs zones Wavelength. Vous pouvez ensuite utiliser AWS des ressources telles que les instances Amazon EC2 pour exécuter des applications nécessitant une latence très faible et une connexion aux AWS services de la région. Pour plus d'informations, consultez la section [Zones AWS Wavelength](#).

Lorsque vous créez des réservations de capacité à la demande, vous pouvez choisir la zone Wavelength et lancer des instances Réserve de capacité dans une zone Wavelength en spécifiant le sous-réseau associé à la zone Wavelength. Une zone Wavelength est représentée par un code de Région AWS suivi d'un identifiant qui indique l'emplacement, par exemple, us-east-1-w11-bos-w1z-1.

Les zones Wavelength ne sont pas disponibles dans toutes les régions. Pour plus d'informations sur les régions qui prennent en charge les zones Wavelength, consultez [Zones Wavelength disponibles](#) dans le Guide du développeur AWS Wavelength .

Considérations

Vous ne pouvez pas utiliser de groupes de Réserve de capacité dans une zone Wavelength.

Pour utiliser une Réserve de capacité dans une zone Wavelength

1. Activez la Wavelength Zone pour l'utiliser dans votre AWS compte. Pour plus d'informations, consultez [the section called "Activer les zones Wavelength"](#).
2. Créez une Réserve de capacité dans la zone Wavelength. Pour Zone de disponibilité, sélectionnez une Wavelength. La Wavelength est représentée par un code de AWS région suivi

- d'un identifiant indiquant l'emplacement, par exemple `us-east-1-w11-bos-w1z-1`. Pour plus d'informations, consultez [Créer une Réserve de capacité](#).
3. Créez un sous-réseau dans la zone Wavelength. Pour Zone de disponibilité, sélectionnez une zone Wavelength. Pour plus d'informations, consultez [Créer un sous-réseau dans votre VPC](#) dans le Guide de l'utilisateur Amazon VPC.
 4. Lancez une instance. Pour Sous-réseau, sélectionnez le sous-réseau dans la zone Wavelength (par exemple, `subnet-123abc | us-east-1-w11-bos-w1z-1`) et, pour Réserve de capacité, sélectionnez la spécification (open ou ciblez-la par ID) requise pour la Réserve de capacité que vous avez créée dans Wavelength. Pour plus d'informations, consultez [Lancer des instances dans une Réserve de capacité existante](#).

Réservations de capacité sur AWS Outposts

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructure, les services, les API et les outils aux locaux des clients. En fournissant un accès local à l'infrastructure AWS gérée, il AWS Outposts permet aux clients de créer et d'exécuter des applications sur site en utilisant les mêmes interfaces de programmation que dans AWS les régions, tout en utilisant les ressources de calcul et de stockage locales pour réduire la latence et les besoins de traitement des données locaux.

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région.

Vous pouvez créer des réservations de capacité sur les Outposts que vous avez créés dans votre compte. Cela vous permet de réserver une capacité de calcul sur un outpost de votre site. Vous créez et utilisez des réservations de capacité dans Outposts de la même manière que vous créez et utilisez des réservations de capacité dans les zones de disponibilité standard. Les fonctionnalités et le comportement de correspondance d'instance sont les mêmes.

Vous pouvez également partager les réservations de capacité sur les Outposts avec d'autres AWS comptes de votre organisation à l'aide de. AWS Resource Access Manager Pour plus d'informations sur le partage des réserves de capacité, consultez [Utiliser des réservations de capacité partagées](#).

Prérequis

Vous devez avoir un outpost installé sur votre site. Pour plus d'informations, consultez [Créer un outpost et commander une capacité outpost](#) dans le Guide de l'utilisateur AWS Outposts .

Considérations

- Vous ne pouvez pas utiliser les groupes de réservation de capacité sur un Outpost.

Pour utiliser une réservation de capacité sur un Outpost.

1. Créez un sous-réseau sur l'outpost. Pour plus d'informations, consultez [Créer un sous-réseau](#) dans le Guide de l'utilisateur AWS Outposts .
2. Créez une réservation de capacité sur l'outpost.
 - a. Ouvrez la AWS Outposts console à l'[adresse https://console.aws.amazon.com/outposts/](https://console.aws.amazon.com/outposts/).
 - b. Dans le volet de navigation, choisissez Outposts, puis choisissez Actions, Créer une réservation de capacité.
 - c. Configurez la réservation de capacité selon vos besoins, puis choisissez Créer. Pour plus d'informations, consultez [Créer une Réserve de capacité](#).

 Note

La liste déroulante Type d'instance répertorie uniquement les types d'instance pris en charge par l'outpost sélectionné, et la liste déroulante Zone de disponibilité répertorie uniquement la zone de disponibilité à laquelle l'outpost sélectionné est associé.

3. Lancez une instance dans la réservation de capacité. Pour Sous-réseau choisissez le sous-réseau que vous avez créé à l'étape 1 et pour Réserve de capacité, sélectionnez la réservation de capacité que vous avez créée à l'étape 2. Pour plus d'informations, consultez la section [Lancer une instance sur votre Outpost](#) du Guide de l'utilisateur AWS Outposts .

Utiliser des réservations de capacité partagées

Le partage des réservations de capacité permet aux propriétaires des réservations de capacité de partager leur capacité réservée avec d'autres AWS comptes ou au sein d'une AWS organisation. Cela vous permet de créer et de gérer les réservations de capacité de manière centralisée, et de partager la capacité réservée entre plusieurs AWS comptes ou au sein de votre AWS organisation.

Dans ce modèle, le AWS compte propriétaire de la réservation de capacité (propriétaire) la partage avec d'autres AWS comptes (consommateurs). Les consommateurs peuvent lancer des instances dans des réservations de capacité partagées avec eux comme ils le feraient avec des réservations de capacité qu'ils possèderaient dans leur propre compte. Le propriétaire d'une Réserve de

capacité est responsable de la gestion de la Réserve de capacité et des instances lancées dans celle-ci. Les propriétaires ne peuvent pas modifier les instances lancées par les consommateurs dans des réservations de capacité qu'ils ont partagées. Les consommateurs sont responsables de la gestion des instances qu'ils lancent dans des réservations de capacité partagées avec eux. Les consommateurs ne peuvent pas voir ou modifier les instances appartenant à d'autres consommateurs ou au propriétaire de la Réserve de capacité.

Un propriétaire de Réserve de capacité peut partager une Réserve de capacité avec :

- AWS Comptes spécifiques à l'intérieur ou à l'extérieur de son AWS organisation
- Une unité organisationnelle au sein de son AWS organisation
- Toute son AWS organisation

Table des matières

- [Conditions préalables au partage de réservations de capacité](#)
- [Services connexes](#)
- [Partager sur plusieurs zones de disponibilité](#)
- [Partager une Réserve de capacité](#)
- [Arrêter de partager une Réserve de capacité](#)
- [Identification et affichage d'une réserve de capacité partagée](#)
- [Afficher l'utilisation de Réserve de capacité partagées](#)
- [Autorisations relatives à une Réserve de capacité partagée](#)
- [Facturation et mesures](#)
- [Limites d'instance](#)

Conditions préalables au partage de réservations de capacité

- Pour partager une réservation de capacité, vous devez la posséder dans votre AWS compte. Vous ne pouvez pas partager une Réserve de capacité qui a été partagée avec vous.
- Vous pouvez uniquement partager des réservations de capacité pour les instances de locations partagées. Vous ne pouvez pas partager de réservations de capacité pour les instances de locations dédiées.
- Le partage des réservations de capacité n'est pas disponible pour AWS les nouveaux AWS comptes ou les comptes dont l'historique de facturation est limité.

- Pour partager une réservation de capacité avec votre AWS organisation ou une unité organisationnelle de votre AWS organisation, vous devez activer le partage avec AWS Organizations. Pour plus d'informations, consultez [Activation du partage avec AWS Organizations](#) dans le Guide de l'utilisateur AWS RAM .

Services connexes

Le partage des réservations de capacité s'intègre à AWS Resource Access Manager (AWS RAM). AWS RAM est un service qui vous permet de partager vos AWS ressources avec n'importe quel AWS compte ou via AWS Organizations. Avec AWS RAM, vous partagez les ressources que vous possédez en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent être AWS des comptes individuels, des unités organisationnelles ou l'ensemble d'une organisation AWS Organizations.

Pour plus d'informations AWS RAM, consultez le [guide de AWS RAM l'utilisateur](#).

Partager sur plusieurs zones de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte. Cela peut entraîner des différences de nom de zone de disponibilité entre les comptes. Par exemple, il est possible que la zone us-east-1a de disponibilité de votre AWS compte ne soit pas la même que celle us-east-1a d'un autre AWS compte.

Pour identifier l'emplacement de vos Réservations de capacité par rapport à vos comptes, vous devez utiliser l'ID de zone de disponibilité. L'AZ ID est un identifiant unique et cohérent pour une zone de disponibilité pour tous les AWS comptes. Par exemple, use1-az1 il s'agit d'un identifiant AZ pour la us-east-1 région et il s'agit du même emplacement dans tous les AWS comptes.

Pour afficher les ID de zone de disponibilité pour votre compte

1. Ouvrez la AWS RAM console à l'[adresse https://console.aws.amazon.com/ram](https://console.aws.amazon.com/ram).
2. Les ID de zone de disponibilité pour la région actuelle sont affichés dans le volet Your AZ ID (Votre ID de zone de disponibilité) dans la partie droite de l'écran.

Partager une Réserve de capacité

Lorsque vous partagez une réserve de capacité dont vous êtes propriétaire avec d'autres AWS comptes, vous leur permettez de lancer des instances dans la capacité que vous avez réservée. Si vous partagez une Réserve de capacité ouverte, gardez présent à l'esprit les points suivants, car cela pourrait entraîner une utilisation indésirable de la Réserve de capacité :

- Si des consommateurs disposent d'instances en cours d'exécution correspondant aux attributs de la Réserve de capacité, du paramètre `CapacityReservationPreference` défini sur `open` et qu'ils ne procèdent pas à l'exécution dans une capacité réservée, ils utilisent automatiquement la Réserve de capacité partagée.
- Si les consommateurs lancent des instances dont les attributs correspondent (type d'instance, plateforme, zone de disponibilité et location) et dont le `CapacityReservationPreference` paramètre est défini sur `open`, ils se lancent automatiquement dans la réserve de capacité partagée.

Pour partager une Réserve de capacité, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une AWS RAM ressource qui vous permet de partager vos ressources entre différents AWS comptes. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Lorsque vous partagez une Réserve de capacité avec la console Amazon EC2, vous l'ajoutez à un partage de ressources existant. Pour ajouter une réserve de capacité à un nouveau partage de ressources, vous devez créer le partage de ressources avec la [console AWS RAM](#).

Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, les clients de votre organisation ont accès à la réserve de capacité partagée si les [conditions préalables au partage](#) sont remplies. Si la réserve de capacité est partagée avec des comptes externes, ils reçoivent une invitation à rejoindre le partage de ressources et bénéficient d'un accès à la réserve de capacité partagée après avoir accepté l'invitation.

Important

Avant de lancer des instances dans une réserve de capacité partagée avec vous, vérifiez que vous avez accès à la réserve de capacité partagée en la visualisant dans la console ou en la décrivant à l'aide de la commande [describe-capacity-reservations](#). AWS CLI Si vous pouvez consulter la réserve de capacité partagée dans la console ou la décrire à l'aide du AWS CLI, elle est disponible pour votre usage et vous pouvez y lancer des instances. Si vous

tentez de lancer des instances dans la réserve de capacité et qu'elle n'est pas accessible en raison d'un échec de partage, les instances seront lancées dans la capacité à la demande.

Vous pouvez partager une réserve de capacité qui vous appartient avec la console Amazon EC2, la console AWS RAM ou la AWS CLI.

Pour partager une réservation de capacité qui vous appartient avec la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Réservations de capacité.
3. Choisissez la Réserve de capacité à partager, puis choisissez Actions, Share reservation (Partager une réservation).
4. Sélectionnez le partage de ressources auquel vous souhaitez ajouter la Réserve de capacité, puis choisissez Share Réserve de capacité (Partager la réservation de capacité).

Les consommateurs peuvent avoir accès à la Réserve de capacité partagée en quelques minutes.

Pour partager une réservation de capacité dont vous êtes propriétaire à l'aide de la AWS RAM console

Consultez [Création d'un partage de ressources](#) dans le Guide de l'utilisateur AWS RAM .

Pour partager une réservation de capacité dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande [create-resource-share](#).

Arrêter de partager une Réserve de capacité

Le propriétaire d'une Réserve de capacité peut cesser de partager une Réserve de capacité à tout moment. Les règles suivantes s'appliquent :

- Les instances appartenant aux consommateurs qui étaient en cours d'exécution dans la capacité partagée au moment où le partage s'arrête continuent de s'exécuter normalement en dehors de la capacité réservée, et la capacité est restaurée dans la Réserve de capacité soumise à la disponibilité de capacité Amazon EC2.
- Les consommateurs avec lesquels la Réserve de capacité était partagée ne peuvent plus lancer de nouvelles instances dans la capacité réservée.

Pour arrêter de partager une Réserve de capacité que vous possédez, vous devez la supprimer du partage de ressources. Pour ce faire, vous pouvez utiliser la console Amazon EC2, la console AWS RAM ou la AWS CLI.

Pour arrêter le partage d'une Réserve de capacité que vous possédez à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Réservations de capacité.
3. Sélectionnez la Réserve de capacité et choisissez l'onglet Sharing (Partage).
4. L'onglet Sharing (Partage) affiche la liste des partages de ressources auxquels la Réserve de capacité a été ajoutée. Sélectionnez le partage de ressources duquel vous souhaitez supprimer la Réserve de capacité, puis choisissez Remove from resource share (Supprimer du partage de ressources).

Pour arrêter de partager une réservation de capacité dont vous êtes propriétaire à l'aide de la AWS RAM console

Consultez [Mise à jour d'un partage de ressources](#) dans le Guide de l'utilisateur AWS RAM .

Pour arrêter de partager une réservation de capacité dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande [disassociate-resource-share](#).

Identification et affichage d'une réserve de capacité partagée

Important

Avant de lancer des instances dans une réserve de capacité partagée avec vous, vérifiez que vous avez accès à la réserve de capacité partagée en l'affichant dans la console ou en la décrivant à l'aide de la commande AWS CLI. Si vous pouvez consulter la réservation de capacité partagée dans la console ou la décrire à l'aide du AWS CLI, elle est disponible pour votre usage et vous pouvez y lancer des instances. Si vous tentez de lancer des instances dans la réserve de capacité et qu'elle n'est pas accessible en raison d'un échec de partage, l'instance sera lancée dans la capacité à la demande.

Les propriétaires et les consommateurs peuvent identifier et visualiser les réserves de capacité partagées à l'aide de la console Amazon EC2 et de l' AWS CLI.

Pour identifier une Réserve de capacité partagée avec la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Réservations de capacité. L'écran affiche la liste des réservations de capacité qui vous appartiennent et des réservations de capacité qui sont partagées avec vous. La colonne Propriétaire indique l'ID de AWS compte du propriétaire de la réservation de capacité. (me) à côté de l'identifiant du AWS compte indique que vous en êtes le propriétaire.

Pour identifier une réservation de capacité partagée à l'aide du AWS CLI

Utilisez la commande [describe-capacity-reservations](#) : La commande renvoie les réservations de capacité que vous possédez et les réservations de capacité partagées avec vous. OwnerId indique l'ID de AWS compte du propriétaire de la réservation de capacité.

Afficher l'utilisation de Réserve de capacité partagées

Le propriétaire d'une réserve de capacité partagée peut afficher à tout moment son utilisation à l'aide de la console Amazon EC2 et de la AWS CLI.

Pour afficher l'utilisation d'une Réserve de capacité à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Réservations de capacité.
3. Sélectionnez la Réserve de capacité dont vous souhaitez voir l'utilisation et choisissez l'onglet Usage (Utilisation).

La colonne AWS account ID (ID de compte) indique l'ID de compte des consommateurs qui utilisent actuellement la réserve de capacité. La colonne Launched instances (Instances lancées) indique le nombre d'instances en cours d'exécution pour chaque consommateur dans la capacité réservée.

Pour consulter l'utilisation des réservations de capacité à l'aide du AWS CLI

Utilisez la commande [get-capacity-reservation-usage](#). AccountId indique l'ID du compte utilisant la Réserve de capacité. UsedInstanceCount indique le nombre d'instances en cours d'exécution pour le consommateur dans la capacité réservée.

Autorisations relatives à une Réserve de capacité partagée

Autorisations accordées aux propriétaires

Les propriétaires sont responsables de la gestion et de l'annulation de leurs réservations de capacité partagées. Les propriétaires ne peuvent pas modifier des instances appartenant à d'autres comptes et en cours d'exécution dans la Réserve de capacité. Les propriétaires sont responsables de la gestion des instances qu'ils lancent dans la Réserve de capacité partagée.

Autorisations accordées aux consommateurs

Les consommateurs sont responsables de la gestion de leurs instances exécutées dans la Réserve de capacité partagée. Les consommateurs ne peuvent pas modifier la Réserve de capacité partagée. Ils ne peuvent pas non plus afficher ou modifier des instances qui appartiennent à d'autres consommateurs ou au propriétaire de la Réserve de capacité.

Facturation et mesures

Le partage de réservations de capacité n'entraîne pas de frais supplémentaires.

Le propriétaire de la Réserve de capacité est facturé pour les instances qu'il exécute dans la Réserve de capacité et pour la capacité réservée non utilisée. Les consommateurs sont facturés pour les instances qu'ils exécutent dans la Réserve de capacité partagée.

Si le propriétaire de la réserve de capacité appartient à un autre compte payeur et que la réserve de capacité est couverte par une instance régionale réservée ou un Savings Plan, le propriétaire de la réserve de capacité continue d'être facturé pour l'instance régionale réservée ou le Savings Plan. Dans ces cas, le propriétaire de la réserve de capacité paie pour l'instance réservée régionale ou le Savings Plan et les consommateurs sont facturés pour les instances qu'ils exécutent dans la réserve de capacité partagée.

Limites d'instance

Toute utilisation d'une Réserve de capacité est prise en compte par rapport aux limites instance à la demande du propriétaire de la Réserve de capacité. Cela comprend :

- La capacité réservée non utilisée
- L'utilisation par des instances qui appartiennent au propriétaire de la Réserve de capacité
- L'utilisation par des instances qui appartiennent aux consommateurs

Les instances lancées dans la capacité partagée par des consommateurs sont prises en compte par rapport à la limite instance à la demande du propriétaire de la Réserve de capacité. Les limites d'instance des consommateurs sont égales à la somme de leurs propres limites instance à la demande et de la capacité disponible dans les réservations de capacité partagées auxquelles ils ont accès.

Flottes de réservation de capacité

Une flotte de réservation de capacité à la demande est un groupe de réservations de capacité.

Une demande de flotte de réservation de capacité contient toutes les informations de configuration nécessaires pour lancer une flotte de réservation de capacité. En une seule demande, vous pouvez réserver de grandes quantités de capacité Amazon EC2 pour votre charge de travail à travers plusieurs types d'instances, jusqu'à une capacité cible que vous spécifiez.

Après avoir créé une flotte de réservation de capacité, vous pouvez gérer collectivement les réservations de capacité de la flotte en modifiant ou en annulant la flotte de réservation de capacité.

Rubriques

- [Fonctionnement de flottes de réservation de capacité](#)
- [Considérations](#)
- [Tarification](#)
- [Concepts des flottes de réservation de capacité](#)
- [Utilisation des flottes de réservation de capacité](#)
- [Exemples de configurations de flotte de réservation de capacité](#)
- [Utilisation des rôles liés à un service pour la flotte de réserve de capacité](#)

Fonctionnement de flottes de réservation de capacité

Lorsque vous créez une flotte de réservation de capacité, celle-ci tente de créer des réservations de capacité individuelles pour atteindre la capacité cible totale que vous avez spécifiée dans la demande de la flotte.

Le nombre d'instances pour lesquelles la flotte réserve de la capacité dépend de la [capacité cible totale](#) et des [pondérations du type d'instance](#) que vous spécifiez. Le type d'instance pour lequel il réserve la capacité dépend de la [stratégie d'allocation](#) et des [priorités de type d'instance](#) que vous utilisez.

Si la capacité est insuffisante au moment de la création de la flotte et qu'elle n'est pas en mesure d'atteindre immédiatement sa capacité cible totale, elle tente de manière asynchrone de créer des réservations de capacité jusqu'à ce qu'elle ait réservé la quantité de capacité demandée.

Lorsque la flotte atteint sa capacité cible totale, elle tente de maintenir cette capacité. Si une réservation de capacité de la flotte est annulée, celle-ci crée automatiquement une ou plusieurs réservations de capacité, selon la configuration de votre flotte, pour remplacer la capacité perdue et maintenir sa capacité cible totale.

Les réservations de capacité dans la flotte ne peuvent pas être gérées individuellement. Elles doivent être gérées collectivement en modifiant la flotte. Lorsque vous modifiez une flotte, les réservations de capacité de celle-ci sont automatiquement mises à jour pour refléter les changements.

Actuellement, les flottes de réservation de capacité prennent en charge le critère de correspondance d'instance open, et toutes les réservations de capacité lancées par une flotte utilisent automatiquement ce critère de correspondance d'instance. Avec ce critère, les nouvelles instances et les instances existantes dont les attributs correspondent (type d'instance, plateforme, zone de disponibilité et location) s'exécutent automatiquement dans les réservations de capacité créées par une flotte. Les flottes de réservation de capacité ne prennent pas en charge les critères de correspondance des instances target.

Considérations

Gardez les points suivants à l'esprit lorsque vous travaillez avec des flottes de réservation de capacité :

- Une flotte de réservation de capacité peut être créée, modifiée, consultée et annulée à l'aide de l'AWS API AWS CLI and.
- Les réservations de capacité dans une flotte ne peuvent pas être gérées individuellement. Elles doivent être gérées collectivement en modifiant ou en annulant la flotte.
- Une flotte de réservation de capacité ne peut pas s'étendre sur plusieurs régions.
- Une flotte de réservation de capacité ne peut pas s'étendre sur plusieurs zones de disponibilité.
- Les réservations de capacité créées par une flotte de réservation de capacité sont automatiquement étiquetées avec le tag AWS généré suivant :
 - Clé : `aws:ec2-capacity-reservation-fleet`
 - Valeur : `fleet_id`

Vous pouvez utiliser cette identification pour identifier les réservations de capacité qui ont été créées par une flotte de réservation de capacité.

Tarifification

L'utilisation des flottes de réservation de capacité ne donne lieu à aucun frais supplémentaire. Vous êtes facturé pour les réservations de capacité individuelles créées par vos flottes de réservation de capacité. Pour plus d'informations sur la façon dont les réservations de capacité sont facturées, consultez [Tarification et facturation d'une Réservation de capacité](#).

Concepts des flottes de réservation de capacité

Cette rubrique décrit certains des concepts des flottes de réservation de capacité.

Rubriques

- [Capacité cible totale](#)
- [Stratégie d'allocation](#)
- [Pondération du type d'instance](#)
- [Priorité de type d'instance](#)

Capacité cible totale

La capacité cible totale définit la quantité totale de capacité de calcul que la flotte de réservation de capacité réserve. Vous spécifiez la capacité cible totale lorsque vous créez la flotte de réservation de capacité. Après la création de la flotte, Amazon EC2 crée automatiquement des réservations de capacité pour réserver la capacité jusqu'à la capacité cible totale.

Le nombre d'instances pour lesquelles la flotte de réservation de capacité réserve de la capacité est déterminé par la capacité cible totale et la pondération du type d'instance que vous spécifiez pour chaque type d'instance dans la flotte de réservation de capacité (`total target capacity/instance type weight=number of instances`).

Vous pouvez attribuer une capacité cible totale en fonction d'unités significatives pour votre charge de travail. Par exemple, si votre charge de travail nécessite un certain nombre de vCPU, vous pouvez attribuer la capacité cible totale en fonction du nombre de vCPU requis. Si votre charge de travail nécessite 2048 vCPU, spécifiez une capacité cible totale de 2048 et attribuez ensuite des

pondérations aux types d'instance en fonction du nombre de vCPU fournis par les types d'instance de la flotte. Pour obtenir un exemple, consultez [Pondération du type d'instance](#).

Stratégie d'allocation

La stratégie d'allocation de votre flotte de réservation de capacité détermine comment elle répond à votre demande de capacité réservée à partir des spécifications du type d'instance dans la configuration de la flotte de réservation de capacité.

Actuellement, seule la stratégie d'allocation `prioritized` est prise en charge. Avec cette stratégie, la flotte de réservation de capacité crée des réservations de capacité en utilisant les priorités que vous avez assignées à chacune des spécifications de type d'instance dans la configuration de la flotte de réservation de capacité. Les valeurs de priorité inférieures indiquent une priorité d'utilisation plus élevée. Par exemple, supposons que vous créez une flotte de réservation de capacité qui utilise les types d'instance et les priorités suivants :

- `m4.16xlarge` — priorité = 1
- `m5.16xlarge` — priorité = 3
- `m5.24xlarge` — priorité = 2

La flotte tente d'abord de créer des réservations de capacité pour `m4.16xlarge`. Si Amazon EC2 ne dispose pas d'une capacité suffisante pour `m4.16xlarge`, la flotte tente de créer des réservations de capacité pour `m5.24xlarge`. Si Amazon EC2 ne dispose pas d'une capacité suffisante pour `m5.24xlarge`, la flotte crée des réservations de capacité pour `m5.16xlarge`.

Pondération du type d'instance

La pondération du type d'instance est une pondération que vous attribuez à chaque type d'instance dans la flotte de réservation de capacité. La pondération détermine combien d'unités de capacité chaque instance de ce type d'instance spécifique compte pour la capacité cible totale de la flotte.

Vous pouvez attribuer des pondérations en fonction des unités qui sont significatives pour votre charge de travail. Par exemple, si votre charge de travail nécessite un certain nombre de vCPU, vous pouvez attribuer des pondérations en fonction du nombre de vCPU fournis par chaque type d'instance de la flotte de réservation de capacité. Dans ce cas, si vous créez une flotte de réservation de capacité utilisant des instances `m4.16xlarge` et `m5.24xlarge`, vous attribuerez des pondérations correspondant au nombre de vCPU de chaque instance comme suit :

- `m4.16xlarge` — 64 vCPUs, poids =64 unités

- `m5.24xlarge` — 96 vCPUs, poids =96 unités

La pondération du type d'instance détermine le nombre d'instances pour lesquelles la flotte de réservation de capacité réserve de la capacité. Par exemple, si une flotte de réservation de capacité ayant une capacité cible totale de 384 unités utilise les types d'instance et les pondérations de l'exemple précédent, la flotte pourrait réserver une capacité pour 6 `m4.16xlarge` instances ($384 \text{ capacité cible totale} / 64 \text{ pondération du type d'instance} = 6 \text{ instances}$), ou 4 `m5.24xlarge` instances ($384 / 96 = 4$).

Si vous n'attribuez pas de pondération aux types d'instance, ou si vous attribuez une pondération de type d'instance de 1, la capacité cible totale est basée uniquement sur le nombre d'instances. Par exemple, si une flotte de réservation de capacité ayant une capacité cible totale de 384 unités utilise les types d'instances de l'exemple précédent, mais omet les pondérations ou spécifie une pondération de 1 pour les deux types d'instances, la flotte pourrait réserver une capacité pour 384 `m4.16xlarge` instances ou 384 `m5.24xlarge` instances.

Priorité de type d'instance

La priorité de type d'instance est une valeur que vous attribuez aux types d'instance de la flotte. Les priorités sont utilisées pour déterminer lequel des types d'instance spécifiés pour la flotte doit être utilisé en priorité.

Les valeurs de priorité inférieures indiquent une priorité d'utilisation plus élevée.

Utilisation des flottes de réservation de capacité

Rubriques

- [Avant de commencer](#)
- [États des flottes de réservation de capacité](#)
- [Création d'une flotte de réservation de capacité](#)
- [Affichage d'une flotte de réservation de capacité](#)
- [Modification d'une flotte de réservation de capacité](#)
- [Annulation d'une flotte de réservation de capacité](#)

Avant de commencer

Avant de créer une flotte de réservation de capacité :

1. Déterminez la quantité de capacité de calcul nécessaire à votre charge de travail.
2. Décidez des types d'instance et des zones de disponibilité que vous voulez utiliser.
3. Attribuez à chaque type d'instance une priorité en fonction de vos besoins et de vos préférences. Pour plus d'informations, consultez [Priorité de type d'instance](#).
4. Créez un système de pondération de la capacité qui a du sens pour votre charge de travail. Attribuez un poids à chaque type d'instance et déterminez votre capacité cible totale. Pour plus d'informations, consultez [Pondération du type d'instance](#) et [Capacité cible totale](#).
5. Déterminez si vous avez besoin de la réservation de capacité indéfiniment ou seulement pour une période de temps spécifique.

États des flottes de réservation de capacité

Une flotte de réservation de capacité peut se trouver dans l'un des états suivants :

- `submitted` — La demande de la flotte de réservation de capacité a été soumise et Amazon EC2 se prépare à créer les réservations de capacité.
- `modifying` — La flotte de réservation de capacité est en cours de modification. La flotte reste dans cet état jusqu'à ce que la modification soit terminée.
- `active` — La flotte de réservation de capacité a atteint sa capacité cible totale et tente de maintenir cette capacité. La flotte reste dans cet état jusqu'à ce qu'elle soit modifiée ou supprimée.
- `partially_fulfilled` — La flotte de réservation de capacité a partiellement atteint sa capacité cible totale. La capacité d'Amazon EC2 est insuffisante pour remplir la capacité cible totale. La flotte tente de remplir de manière asynchrone sa capacité cible totale.
- `expiring` — La flotte de réservation de capacité a atteint sa date de fin et est en train d'expirer. Une ou plusieurs de ses réservations de capacité peuvent encore être actives.
- `expired` — La flotte de réservation de capacité a atteint sa date d'expiration. La flotte et ses réservations de capacité sont expirées. La flotte ne peut pas créer de nouvelles réservations de capacité.
- `cancelling` — La flotte de réservation de capacité est en cours d'annulation. Une ou plusieurs de ses réservations de capacité peuvent encore être actives.
- `cancelled` — La flotte de réservation de capacité a été annulée manuellement. La flotte et ses réservations de capacité sont annulées et la flotte ne peut pas créer de nouvelles réservations de capacité.

- **failed** — La flotte de réservation de capacité n'a pas réussi à réserver de la capacité pour les types d'instance spécifiés.

Création d'une flotte de réservation de capacité

Lorsque vous créez une flotte de réservation de capacité, elle crée automatiquement des réservations de capacité pour les types d'instance spécifiés dans la demande de flotte, jusqu'à la capacité cible totale spécifiée. Le nombre d'instances pour lesquelles la flotte de réservation de capacité réserve de la capacité dépend de la capacité cible totale et des pondérations de type d'instance que vous spécifiez dans la demande. Pour plus d'informations, consultez [Pondération du type d'instance](#) et [Capacité cible totale](#).

Lorsque vous créez la flotte, vous devez spécifier les types d'instance à utiliser et une priorité pour chacun de ces types d'instance. Pour plus d'informations, consultez [Stratégie d'allocation](#) et [Priorité de type d'instance](#).

Note

Le rôle `AWSServiceRoleForEC2CapacityReservationFleet` au service est automatiquement créé dans votre compte la première fois que vous créez une flotte de réservation de capacité. Pour plus d'informations, consultez [Utilisation des rôles liés à un service pour la flotte de réserve de capacité](#).

Actuellement, les flottes de réservation de capacité ne prennent en charge que les critères de correspondance de l'instance open.

Vous pouvez créer une flotte de réservation de capacité en utilisant la ligne de commande uniquement.

Pour créer une flotte de réservation de capacité

Utilisez la commande [create-capacity reservation-fleet](#). AWS CLI

```
aws ec2 create-capacity-reservation-fleet \  
--total-target-capacity capacity_units \  
--allocation-strategy prioritized \  
--instance-match-criteria open \  
--tenancy dedicated/default \  
--end-date yyyy-mm-ddThh:mm:ss.000Z \  

```

```
--instance-type-specifications file://instanceTypeSpecification.json
```

Voici le contenu de `instanceTypeSpecification.json`.

```
[
  {
    "InstanceType": "instance_type",
    "InstancePlatform": "platform",
    "Weight": instance_type_weight,
    "AvailabilityZone": "availability_zone",
    "AvailabilityZoneId" : "az_id",
    "EbsOptimized": true/false,
    "Priority" : instance_type_priority
  }
]
```

Sortie attendue.

```
{
  "Status": "status",
  "TotalFulfilledCapacity": fulfilled_capacity,
  "CapacityReservationFleetId": "cr_fleet_id",
  "TotalTargetCapacity": capacity_units
}
```

Exemple

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 24 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-12-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

`instanceTypeSpecification.json`

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "Weight": 3.0,
  }
]
```

```
"AvailabilityZone": "us-east-1a",
"EbsOptimized": true,
"Priority" : 1
}
]
```

Exemple de sortie.

```
{
  "Status": "submitted",
  "TotalFulfilledCapacity": 0.0,
  "CapacityReservationFleetId": "crf-abcdef01234567890",
  "TotalTargetCapacity": 24
}
```

Affichage d'une flotte de réservation de capacité

Vous pouvez afficher les informations de configuration et de capacité d'une flotte de réservation de capacité à tout moment. L'affichage d'une flotte fournit également des détails sur les réservations de capacité individuelles qui se trouvent dans la flotte.

Vous pouvez afficher une flotte de réservation de capacité en utilisant la ligne de commande uniquement.

Pour afficher une flotte de réservation de capacité

Utilisez la commande [describe-capacity reservation-fleets](#). AWS CLI

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Sortie attendue

```
{
  "CapacityReservationFleets": [
    {
      "Status": "status",
      "EndDate": "yyyy-mm-ddThh:mm:ss.000Z",
      "InstanceMatchCriteria": "open",
      "Tags": [],
      "CapacityReservationFleetId": "cr_fleet_id",
      "Tenancy": "dedicated/default",
```

```

    "InstanceTypeSpecifications": [
      {
        "CapacityReservationId": "cr1_id",
        "AvailabilityZone": "cr1_availability_zone",
        "FulfilledCapacity": cr1_used_capacity,
        "Weight": cr1_instance_type_weight,
        "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
        "InstancePlatform": "cr1_platform",
        "TotalInstanceCount": cr1_number_of_instances,
        "Priority": cr1_instance_type_priority,
        "EbsOptimized": true/false,
        "InstanceType": "cr1_instance_type"
      },
      {
        "CapacityReservationId": "cr2_id",
        "AvailabilityZone": "cr2_availability_zone",
        "FulfilledCapacity": cr2_used_capacity,
        "Weight": cr2_instance_type_weight,
        "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
        "InstancePlatform": "cr2_platform",
        "TotalInstanceCount": cr2_number_of_instances,
        "Priority": cr2_instance_type_priority,
        "EbsOptimized": true/false,
        "InstanceType": "cr2_instance_type"
      },
    ],
    "TotalTargetCapacity": total_target_capacity,
    "TotalFulfilledCapacity": total_target_capacity,
    "CreateTime": "yyyy-mm-ddThh:mm:ss.000Z",
    "AllocationStrategy": "prioritized"
  }
]
}

```

Exemple

```

aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890

```

Exemple de sortie

```

{
  "CapacityReservationFleets": [

```

```
{
  "Status": "active",
  "EndDate": "2021-12-31T23:59:59.000Z",
  "InstanceMatchCriteria": "open",
  "Tags": [],
  "CapacityReservationFleetId": "crf-abcdef01234567890",
  "Tenancy": "default",
  "InstanceTypeSpecifications": [
    {
      "CapacityReservationId": "cr-1234567890abcdef0",
      "AvailabilityZone": "us-east-1a",
      "FulfilledCapacity": 5.0,
      "Weight": 1.0,
      "CreateDate": "2021-07-02T08:34:33.398Z",
      "InstancePlatform": "Linux/UNIX",
      "TotalInstanceCount": 5,
      "Priority": 1,
      "EbsOptimized": true,
      "InstanceType": "m5.xlarge"
    }
  ],
  "TotalTargetCapacity": 5,
  "TotalFulfilledCapacity": 5.0,
  "CreateTime": "2021-07-02T08:34:33.397Z",
  "AllocationStrategy": "prioritized"
}
```

Modification d'une flotte de réservation de capacité

Vous pouvez modifier la capacité cible totale et la date d'une flotte de réservation de capacité à tout moment. Lorsque vous modifiez la capacité totale cible d'une flotte de réservation de capacité, la flotte crée automatiquement de nouvelles réservations de capacité, ou modifie ou annule les réservations de capacité existantes dans la flotte pour répondre à la nouvelle capacité totale cible. Lorsque vous modifiez la date de fin de la flotte, les dates de fin de toutes les réservations de capacité individuelles sont mises à jour en conséquence.

Après avoir modifié une flotte, son statut passe à `modifying`. Vous ne pouvez pas tenter d'apporter d'autres modifications à une flotte lorsqu'elle se trouve dans l'état `modifying`.

Vous ne pouvez pas modifier la location, la zone de disponibilité, les types d'instance, les plateformes d'instance, les priorités ou les pondérations utilisées par une flotte de réservation de capacité. Si vous

devez modifier l'un de ces paramètres, vous devrez peut-être annuler la flotte existante et en créer une nouvelle avec les paramètres requis.

Vous pouvez modifier une flotte de réservation de capacité en utilisant la ligne de commande uniquement.

Pour modifier une flotte de réservation de capacité

Utilisez la commande [AWS CLI modify-capacity](#) reservation-fleet.

Note

Vous ne pouvez pas spécifier `--end-date` et `--remove-end-date` dans la même commande.

```
aws ec2 modify-capacity-reservation-fleet \  
--capacity-reservation-fleet-id cr_fleet_ids \  
--total-target-capacity capacity_units \  
--end-date yyyy-mm-ddThh:mm:ss.000Z \  
--remove-end-date
```

Sortie attendue

```
{  
  "Return": true  
}
```

Exemple : Modifier la capacité cible totale

```
aws ec2 modify-capacity-reservation-fleet \  
--capacity-reservation-fleet-id crf-01234567890abcdef \  
--total-target-capacity 160
```

Exemple : Modifier la date de fin

```
aws ec2 modify-capacity-reservation-fleet \  
--capacity-reservation-fleet-id crf-01234567890abcdef \  
--end-date 2021-07-04T23:59:59.000Z
```

Exemple : Supprimer la date de fin

```
aws ec2 modify-capacity-reservation-fleet \  
--capacity-reservation-fleet-id crf-01234567890abcdef \  
--remove-end-date
```

Exemple de sortie

```
{  
  "Return": true  
}
```

Annulation d'une flotte de réservation de capacité

Lorsque vous n'avez plus besoin d'une flotte de réservation de capacité et de la capacité qu'elle réserve, vous pouvez l'annuler. Lorsque vous annulez une flotte, son statut passe à `cancelled` et elle ne peut plus créer de nouvelles réservations de capacité. En outre, toutes les réservations de capacité individuelles de la flotte sont annulées et les instances qui fonctionnaient auparavant dans la capacité réservée continuent de fonctionner normalement dans la capacité partagée.

Vous pouvez annuler une flotte de réservation de capacité en utilisant la ligne de commande uniquement.

Pour annuler une flotte de réservation de capacité

Utilisez la commande [cancel-capacity reservation-fleet](#). AWS CLI

```
aws ec2 cancel-capacity-reservation-fleets \  
--capacity-reservation-fleet-ids cr_fleet_ids
```

Sortie attendue

```
{  
  "SuccessfulFleetCancellations": [  
    {  
      "CurrentFleetState": "state",  
      "PreviousFleetState": "state",  
      "CapacityReservationFleetId": "cr_fleet_id_1"  
    },  
    {  
      "CurrentFleetState": "state",  
      "PreviousFleetState": "state",  
      "CapacityReservationFleetId": "cr_fleet_id_2"  
    }  
  ]  
}
```

```

    ],
    "FailedFleetCancellations": [
      {
        "CapacityReservationFleetId": "cr_fleet_id_3",
        "CancelCapacityReservationFleetError": [
          {
            "Code": "code",
            "Message": "message"
          }
        ]
      }
    ]
  }
}

```

Exemple : Annulation réussie

```

aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890

```

Exemple de sortie

```

{
  "SuccessfulFleetCancellations": [
    {
      "CurrentFleetState": "cancelling",
      "PreviousFleetState": "active",
      "CapacityReservationFleetId": "crf-abcdef01234567890"
    }
  ],
  "FailedFleetCancellations": []
}

```

Exemples de configurations de flotte de réservation de capacité

Rubriques

- [Exemple 1 : Réserver la capacité en fonction des vCPUs](#)

Exemple 1 : Réserver la capacité en fonction des vCPUs

L'exemple suivant crée une flotte de réservation de capacité qui utilise deux types d'instance : m5.4xlarge et m5.12xlarge.

Elle utilise un système de pondération basé sur le nombre de vCPUs fournis par les types d'instance spécifiés. La capacité cible totale est 480 vCPUs. `m5.4xlarge` fournit 16 vCPUs et obtient une pondération de 16, tandis que `m5.12xlarge` fournit 48 vCPUs et obtient une pondération de 48. Ce système de pondération configure la flotte de réservation de capacité pour réserver la capacité soit pour 30 instances `m5.4xlarge` ($480/16=30$), soit pour 10 instances `m5.12xlarge` ($480/48=10$).

La flotte est configurée pour donner la priorité à la capacité de `m5.12xlarge` et obtient la priorité de 1, tandis que `m5.4xlarge` obtient une priorité inférieure de 2. Cela signifie que la flotte tentera de réserver la capacité de `m5.12xlarge` en premier lieu, et ne tentera de réserver la capacité de `m5.4xlarge` que si Amazon EC2 n'a pas suffisamment de capacité de `m5.12xlarge`.

La flotte réserve la capacité pour des instances Windows et la réservation expire automatiquement le `October 31, 2021 à 23:59:59 UTC`.

```
aws ec2 create-capacity-reservation-fleet \  
--total-target-capacity 480 \  
--allocation-strategy prioritized \  
--instance-match-criteria open \  
--tenancy default \  
--end-date 2021-10-31T23:59:59.000Z \  
--instance-type-specifications file://instanceTypeSpecification.json
```

Voici le contenu de `instanceTypeSpecification.json`.

```
[  
  {  
    "InstanceType": "m5.4xlarge",  
    "InstancePlatform": "Windows",  
    "Weight": 16,  
    "AvailabilityZone": "us-east-1a",  
    "EbsOptimized": true,  
    "Priority" : 2  
  },  
  {  
    "InstanceType": "m5.12xlarge",  
    "InstancePlatform": "Windows",  
    "Weight": 48,  
    "AvailabilityZone": "us-east-1a",  
    "EbsOptimized": true,  
    "Priority" : 1  
  }  
]
```

]

Utilisation des rôles liés à un service pour la flotte de réserve de capacité

La flotte de réservation de capacité à la demande utilise des rôles [liés au service AWS Identity and Access Management](#) (IAM). Un rôle lié à un service est un type unique de rôle IAM qui est lié directement à la flotte de réservation de capacité. Les rôles liés au service sont prédéfinis par Capacity Reservation Fleet et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de la flotte de réservation de capacité, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. La flotte de réservation de capacité définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seule la flotte de réservation de capacité peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources de la flotte de réservation de capacité sont ainsi protégées, car vous ne pouvez pas supprimer par inadvertance les autorisations d'accès aux ressources.

Autorisations de rôles liés à un service pour la flotte de réserve de capacité

La flotte de réservation de capacité utilise le rôle lié au service nommé `AWSServiceRoleForEC2CapacityReservationFleet` pour créer, décrire, modifier et annuler les réservations de capacité précédemment créées par une flotte de réservation de capacité, en votre nom.

Le rôle `AWSServiceRoleForEC2CapacityReservationFleet` lié au service fait confiance à l'entité suivante pour assumer le rôle `::capacity-reservation-fleet.amazonaws.com`

Le rôle utilise la `AWSEC2CapacityReservationFleetRolePolicy` politique, qui inclut les autorisations suivantes :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```

    "Action": [
      "ec2:DescribeCapacityReservations",
      "ec2:DescribeInstances"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateCapacityReservation",
      "ec2:CancelCapacityReservation",
      "ec2:ModifyCapacityReservation"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:capacity-reservation/*"
    ],
    "Condition": {
      "StringLike": {
        "ec2:CapacityReservationFleet": "arn:aws:ec2:*:*:capacity-
reservation-fleet/crf-*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:capacity-reservation/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": "CreateCapacityReservation"
      }
    }
  }
]
}

```

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour la flotte de réserve de capacité

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une flotte de réservation de capacité à l'aide de la `create-capacity-reservation-fleet` AWS CLI commande ou de l'`CreateCapacityReservationFleetAPI`, le rôle lié au service est automatiquement créé pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez une flotte de réservation de capacité, elle crée à nouveau le rôle lié à un service pour vous.

Modification d'un rôle lié à un service pour la flotte de réserve de capacité

La flotte de réservation de capacité ne vous permet pas de modifier le rôle `AWSServiceRoleForEC2CapacityReservationFleet` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour la flotte de réserve de capacité

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez supprimer les ressources de votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Note

Si le service de la flotte de réservation de capacité utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer le rôle lié à `AWSServiceRoleForEC2CapacityReservationFleet` un service

1. Utilisez la `delete-capacity-reservation-fleet` AWS CLI commande ou l'`DeleteCapacityReservationFleetAPI` pour supprimer les flottes de réservation de capacité de votre compte.

2. Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForEC2CapacityReservationFleet` service. Pour plus d'informations, consultez [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service de la flotte de réserve de capacité de capacité

La flotte de réservation de capacité prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez [Régions et Points de terminaison AWS](#).

Surveillance des réserves de capacité

Vous pouvez utiliser les fonctionnalités suivantes pour surveiller vos réserves de capacité :

Rubriques

- [Surveillez les réservations de capacité à l'aide de CloudWatch métriques](#)
- [Surveillez les réservations de capacité à l'aide EventBridge](#)
- [Notifications d'utilisation](#)

Surveillez les réservations de capacité à l'aide de CloudWatch métriques

Grâce aux CloudWatch métriques, vous pouvez surveiller efficacement vos réservations de capacité et identifier les capacités inutilisées en configurant des CloudWatch alarmes pour vous avertir lorsque les seuils d'utilisation sont atteints. Cela peut vous aider à maintenir un volume de Réservation de capacité constant et à atteindre un niveau d'utilisation plus élevé.

Les réservations de capacité à la demande envoient des données métriques CloudWatch toutes les cinq minutes. Les métriques ne sont pas prises en charge pour des réservations de capacité qui sont actives pendant moins de cinq minutes.

Pour plus d'informations sur l'affichage des métriques dans la CloudWatch console, consultez la section [Utilisation d'Amazon CloudWatch Metrics](#). Pour plus d'informations sur la création d'alarmes, consultez [Creating Amazon CloudWatch Alarms](#).

Table des matières

- [Métriques d'utilisation Réservation de capacité](#)
- [Dimensions de métriques Réservation de capacité](#)

- [Afficher CloudWatch les statistiques relatives aux réservations de capacité](#)

Métriques d'utilisation Réserve de capacité

L'espace de nom `AWS/EC2CapacityReservations` inclut les mesures d'utilisation suivantes que vous pouvez employer pour surveiller et maintenir la capacité à la demande à l'intérieur des seuils que vous spécifiez pour votre réservation.

Métrique	Description
<code>UsedInstanceCount</code>	Nombre d'instances actuellement utilisées. Unité : nombre
<code>AvailableInstanceCount</code>	Nombre d'instances qui sont disponibles. Unité : nombre
<code>TotalInstanceCount</code>	Nombre total d'instances que vous avez réservées. Unité : nombre
<code>InstanceUtilization</code>	Pourcentage d'instances de capacité réservées qui sont actuellement utilisées. Unité : pourcentage

Dimensions de métriques Réserve de capacité

Vous pouvez utiliser les dimensions suivantes pour affiner les métriques répertoriées dans les tableaux précédents.

Dimension	Description
<code>CapacityReservationId</code>	

Dimension	Description
	Cette dimension globalement unique filtre uniquement les données que vous demandez pour la réservation de capacité identifiée.

Afficher CloudWatch les statistiques relatives aux réservations de capacité

Les métriques sont d'abord regroupées par espaces de noms de service, puis par dimensions prises en charge. Vous pouvez utiliser les procédures ci-dessous pour afficher les métriques pour vos réservations de capacité.

Pour consulter les statistiques de réservation de capacité à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Si nécessaire, changez la région. Dans la barre de navigation, sélectionnez la région où réside la Réserve de capacité. Pour plus d'informations, consultez [Régions et points de terminaison](#).
3. Dans le volet de navigation, sélectionnez Metrics (Métriques).
4. Pour Toutes les mesures, choisissez Réservations de capacité EC2.
5. Choisissez la dimension de métrique Par réservation de capacité. Les métriques seront regroupées par CapacityReservationId.
6. Pour trier les métriques, utilisez l'en-tête de colonne. Pour représenter graphiquement une métrique, cochez la case en regard de la métrique.

Pour afficher les métriques de réserve de capacité (AWS CLI)

Utilisez la commande [list-metrics](#) suivante :

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Surveillez les réservations de capacité à l'aide EventBridge

AWS Health envoie des événements à Amazon EventBridge lorsqu'une réservation de capacité enregistrée sur votre compte est inférieure à 20 % d'utilisation sur certaines périodes. Avec EventBridge, vous pouvez établir des règles qui déclenchent des actions programmées en réponse à de tels événements. Par exemple, vous pouvez créer une règle qui annule

automatiquement une réserve de capacité lorsque son taux d'utilisation passe en dessous de 20 % sur une période de 7 jours.

Les événements dans EventBridge sont représentés sous forme d'objets JSON. Les champs spécifiques à l'événement figurent dans la section « détail » de l'objet JSON. Le champ « événement » contient le nom de l'événement. Le champ « résultat » contient l'état terminé de l'action qui déclenche l'événement. Pour plus d'informations, consultez les [modèles EventBridge d'événements Amazon](#) dans le guide de EventBridge l'utilisateur Amazon.

Pour plus d'informations, consultez le [guide de EventBridge l'utilisateur Amazon](#).

Cette fonctionnalité n'est pas prise en charge dans AWS GovCloud (US).

Table des matières

- [Événements](#)
- [Création d'une EventBridge règle](#)

Événements

AWS Health envoie les événements suivants lorsque l'utilisation de la capacité pour une réservation de capacité est inférieure à 20 %.

Événements

- [AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION](#)
- [AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY](#)

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION

Voici un exemple d'événement généré lorsqu'une réserve de capacité nouvellement créée a un taux d'utilisation de la capacité inférieur à 20 % sur une période de 24 heures.

```
{
  "version": "0",
  "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2023-03-10T12:03:38Z",
```

```

"region": "ap-south-1",
"resources": [
  "cr-01234567890abcdef"
],
"detail": {
  "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
  "service": "EC2",
  "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
  "eventTypeCategory": "accountNotification",
  "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
  "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
  "eventDescription": [
    {
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }
  ],
  "affectedEntities": [
    {
      "entityValue": "cr-01234567890abcdef"
    }
  ]
}
}

```

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

Voici un exemple d'événement généré lorsqu'une ou plusieurs réserves de capacité nouvellement créées ont un taux d'utilisation de la capacité inférieur à 20 % sur une période de 7 jours.

```

{
  "version": "0", "id": "7439d42b-3c7f-ad50-6a88-25e2a70977e2",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2023-03-07T06:06:01Z",
  "region": "us-east-1",
  "resources": [
    "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
    "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
  ],

```

```

    "detail": {
      "eventArn": "arn:aws:health:us-east-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
      "service": "EC2",
      "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
      "eventTypeCategory": "accountNotification",
      "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
      "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
      "eventDescription": [
        {
          "language": "en_US",
          "latestDescription": "A description of the event will be provided
here"
        }
      ],
      "affectedEntities": [
        {
          "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/
UNIX | 0.0%"
        },
        {
          "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/
UNIX | 0.0%"
        }
      ]
    }
  }
}

```

Création d'une EventBridge règle

Pour recevoir des notifications par e-mail lorsque le taux d'utilisation de votre réservation de capacité tombe en dessous de 20 %, créez une rubrique Amazon SNS, puis une EventBridge règle pour l'`AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION` événement.

Pour créer la rubrique Amazon SNS

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans le panneau de navigation, choisissez Rubriques, puis Créer une rubrique.
3. Pour Type, choisissez Standard.

4. Pour Nom, attribuez un nom à la nouvelle rubrique.
5. Choisissez Créer une rubrique.
6. Choisissez Créer un abonnement.
7. Pour Protocole, choisissez E-mail, puis pour Point de terminaison, saisissez l'adresse e-mail qui reçoit les notifications.
8. Choisissez Créer un abonnement.
9. L'adresse e-mail saisie ci-dessus recevra un e-mail avec l'objet suivant : AWS Notification - Subscription Confirmation. Suivez les instructions pour confirmer votre abonnement.

Pour créer la EventBridge règle

1. Ouvrez la EventBridge console Amazon à l'[adresse https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Dans le volet de navigation, sélectionnez Rules (Règles), puis Create rule (Créer une règle).
3. Pour Nom, attribuez un nom à la nouvelle règle.
4. Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
5. Choisissez Suivant.
6. Pour Modèle d'événement, procédez comme suit :
 - a. Pour Event source (Origine de l'événement), choisissez AWS services (Services).
 - b. Pour Service AWS, choisissez AWS Health.
 - c. Pour Type d'événement, choisissez Notification de sous-utilisation des réserves de capacité à la demande EC2.
7. Choisissez Suivant.
8. Pour Cible 1, procédez comme suit :
 - a. Pour Types de cibles, choisissez service AWS.
 - b. Pour Sélectionner une cible, choisissez Rubrique SNS.
 - c. Pour Rubrique, choisissez la rubrique que vous avez créée précédemment.
9. Choisissez Suivant, puis de nouveau Suivant.
10. Choisissez Créer une règle.

Notifications d'utilisation

AWS Health envoie l'e-mail et les AWS Health Dashboard notifications suivants lorsque le taux d'utilisation des capacités pour les réservations de capacité de votre compte tombe en dessous de 20 %.

- Notifications individuelles pour chaque réserve de capacité nouvellement créée dont le taux d'utilisation a été inférieur à 20 % au cours des dernières 24 heures.
- Une notification récapitulative pour toutes les réserves de capacité dont le taux d'utilisation a été inférieur à 20 % au cours des 7 derniers jours.

Les notifications par e-mail et les AWS Health Dashboard notifications sont envoyées à l'adresse e-mail associée au AWS compte propriétaire des réservations de capacité. Les notifications comprennent les informations suivantes :

- L'ID de la capacité de réservation.
- Zone de disponibilité de la réserve de capacité.
- Taux d'utilisation moyen de la réserve de capacité.
- Type d'instance et plateforme (système d'exploitation) de la réserve de capacité.

En outre, lorsque le taux d'utilisation de la capacité pour une réservation de capacité de votre compte tombe en dessous de 20 % sur une période de 24 heures et 7 jours, AWS Health envoie des événements à EventBridge. Avec EventBridge, vous pouvez créer des règles qui activent des actions automatiques, telles que l'envoi de notifications par e-mail ou le déclenchement de AWS Lambda fonctions, en réponse à de tels événements. Pour plus d'informations, consultez [Surveillez les réservations de capacité à l'aide EventBridge](#).

Blocs de capacité pour ML

Les blocs de capacité pour ML vous permettent de réserver des instances GPU très recherchées à une date ultérieure pour prendre en charge vos charges de travail de machine learning (ML) de courte durée. Les instances qui s'exécutent au sein d'un bloc de capacité sont automatiquement placées à proximité les unes des autres dans [Amazon EC2 UltraClusters](#), pour une mise en réseau non bloquante à faible latence, à l'échelle du pétabit.

Avec les blocs de capacité, vous pouvez voir quand la capacité de l'instance GPU sera disponible à des dates ultérieures, et vous pouvez planifier le démarrage d'un bloc de capacité au moment qui

vous convient le mieux. Lorsque vous réservez un bloc de capacité, vous bénéficiez d'une assurance de capacité prévisible pour les instances GPU tout en ne payant que pour le temps dont vous avez besoin. Nous recommandons les blocs de capacité lorsque vous avez besoin d'instances GPU pour prendre en charge vos charges de travail de ML pendant des jours ou des semaines d'affilée et que vous ne souhaitez pas payer pour une réservation lorsque vos instances GPU ne sont pas utilisées.

Voici quelques cas d'utilisation courants des blocs de capacité.

- Entraînement et optimisation du modèle de ML : bénéficiez d'un accès ininterrompu aux instances GPU que vous avez réservées pour terminer l'entraînement et l'optimisation du modèle de machine learning.
- Expérimentations et prototypes de machine learning : exécutez des expériences et créez des prototypes qui nécessitent des instances de GPU pendant de courtes durées.

Les blocs de capacité sont actuellement disponibles pour p5.48xlarge et pour p4d.24xlarge les instances. Les p5.48xlarge instances sont disponibles dans les régions de l'est des États-Unis (Ohio) et de l'est des États-Unis (Virginie du Nord). Les p4d.24xlarge instances sont disponibles dans les régions de l'est des États-Unis (Ohio) et de l'ouest des États-Unis (Oregon). Vous pouvez réserver un bloc de capacité avec un démarrage ultérieur, jusqu'à huit semaines plus tard.

Vous pouvez utiliser les blocs de capacité pour réserver p5 des p4d instances avec les options de durée de réservation et de quantité d'instances suivantes.

- Durée des réservations par incrément d'un jour, pouvant aller jusqu'à 14 jours au total
- Options de quantité d'instances des réservations pour 1, 2, 4, 8, 16, 32 ou 64 instances

Pour réserver un bloc de capacité, vous devez commencer par spécifier vos besoins en matière de capacité, notamment le type d'instance, le nombre d'instances, la durée, la date de début la plus ancienne et la dernière date de fin dont vous avez besoin. Ensuite, vous pouvez voir une offre de blocs de capacité disponible qui répond à vos spécifications. L'offre de bloc de capacité inclut des informations telles que l'heure de début, la zone de disponibilité et le prix de réservation. Le prix d'une offre de bloc de capacité dépend de l'offre et de la demande au moment où l'offre est proposée. Une fois que vous avez réservé un bloc de capacité, le prix ne change pas. Pour plus d'informations, consultez [Tarification et facturation des blocs de capacité](#).

Lorsque vous achetez un bloc de capacité, votre réservation est créée pour la date et le nombre d'instances que vous avez sélectionnés. Lorsque votre réservation de bloc de capacité commence,

vous pouvez cibler les lancements d'instances en spécifiant l'ID de réservation dans vos demandes de lancement.

Vous pouvez utiliser toutes les instances que vous avez réservées jusqu'à 30 minutes avant la fin du bloc de capacité. Lorsqu'il ne reste que 30 minutes de réservation à votre bloc de capacité, nous commençons à mettre fin à toutes les instances en cours d'exécution dans le bloc de capacité. Nous utilisons ce temps pour nettoyer vos instances avant de livrer le bloc de capacité au client suivant. Les 30 dernières minutes de la réservation ne sont pas incluses dans le prix du bloc de capacité. Nous émettons un événement EventBridge 10 minutes avant le début du processus de résiliation. Pour plus d'informations, consultez [Surveillez les blocs de capacité avec EventBridge](#).

Rubriques

- [Plateformes prises en charge](#)
- [Considérations](#)
- [Ressources connexes](#)
- [Tarification et facturation des blocs de capacité](#)
- [Utiliser des blocs de capacité](#)
- [Surveiller les blocs de capacité](#)

Plateformes prises en charge

Les blocs de capacité pour le ML sont actuellement pris en charge p5.48xlarge et p4d.24xlarge les instances sont louées par défaut. Lorsque vous utilisez le AWS Management Console pour acheter un bloc de capacité, l'option de plate-forme par défaut est Linux/UNIX. Lorsque vous utilisez le AWS Command Line Interface (AWS CLI) ou que AWS SDK vous achetez un bloc de capacité, les options de plateforme suivantes sont disponibles :

- Linux/Unix
- Utilisation de Red Hat Enterprise Linux
- RHEL avec HA
- SUSE Linux
- Ubuntu Pro

Considérations

Avant d'utiliser les blocs de capacité, tenez compte des informations et des limites suivantes.

- Les blocs de capacité commencent et se terminent à 11 h 30, heure universelle coordonnée (UTC).
- Le processus de résiliation pour les instances exécutées dans un bloc de capacité commence à 11 h 00, heure universelle coordonnée (UTC), le dernier jour de la réservation.
- Les blocs de capacité peuvent être réservés avec un démarrage ultérieur, jusqu'à huit semaines plus tard.
- Vous n'êtes pas autorisé à modifier ou annuler les blocs de capacité.
- Les blocs de capacité ne peuvent pas être partagés entre les AWS comptes ou au sein de votre AWS organisation.
- Les blocs de capacité ne peuvent pas être utilisés dans un groupe de réserve de capacité.
- Le nombre total d'instances pouvant être réservées dans les blocs de capacité sur tous les comptes de votre AWS organisation ne peut pas dépasser 64 instances à une date donnée.
- Pour utiliser un bloc de capacité, les instances doivent cibler spécifiquement l'ID de réservation.
- Les instances d'un bloc de capacité ne sont pas prises en compte dans vos limites d'instances à la demande.
- Pour les instances P5 utilisant une AMI personnalisée, assurez-vous de disposer du [logiciel et de la configuration requis pour EFA](#).
- Les blocs de capacité ne peuvent actuellement pas être utilisés avec les groupes de nœuds gérés par Amazon EKS ou Karpenter. Pour plus d'informations sur la création d'un groupe de nœuds autogéré Amazon EKS, consultez [Capacity Blocks for ML](#) dans le guide de l'utilisateur Amazon EKS.

Ressources connexes

Après avoir créé un bloc de capacité, vous pouvez effectuer les opérations suivantes avec le bloc de capacité :

- Lancez des instances dans le bloc de capacité. Pour plus d'informations, consultez [Lancer des instances dans des blocs de capacité](#).
- Créez un groupe Amazon EC2 Auto Scaling. Pour plus d'informations, consultez la section [Utiliser les blocs de capacité pour les charges de travail d'apprentissage automatique](#) dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

Note

Si vous utilisez Amazon EC2 Auto Scaling ou Amazon EKS, vous pouvez planifier le dimensionnement pour qu'il soit exécuté au début de la réservation du Capacity Block. Grâce au dimensionnement planifié, il gère AWS automatiquement les nouvelles tentatives pour vous. Vous n'avez donc pas à vous soucier de la mise en œuvre d'une logique de nouvelles tentatives pour gérer les échecs transitoires.

- Améliorez les flux de travail ML avec AWS ParallelCluster. Pour plus d'informations, consultez [la section Amélioration des flux de travail ML avec AWS ParallelCluster des blocs de capacité Amazon EC2 pour le ML](#).

Pour plus d'informations AWS ParallelCluster, voir [Qu'est-ce que AWS ParallelCluster](#).

Tarification et facturation des blocs de capacité

Rubriques

- [Tarification](#)
- [Facturation](#)

Tarification

Avec les blocs de capacité pour ML Amazon EC2, vous ne payez que ce que vous réservez. Le prix d'un bloc de capacité dépend de l'offre et de la demande des blocs de capacité au moment de l'achat. Vous pouvez afficher le prix d'une offre de bloc de capacité avant de la réserver. Le prix du bloc de capacité est facturé d'avance au moment de la réservation. Lorsque vous recherchez un bloc de capacité sur une plage de dates, nous vous renvoyons l'offre de bloc de capacité la moins chère disponible. Une fois que vous avez réservé un bloc de capacité, le prix ne change pas.

Lorsque vous utilisez un bloc de capacité, vous payez pour le système d'exploitation que vous utilisez lorsque vos instances sont exécutées. Pour plus d'informations sur les prix des systèmes d'exploitation, consultez la section [Amazon EC2 Capacity Blocks for ML Pricing](#).

Facturation

Le prix d'une offre de bloc de capacité est facturé d'avance. Le paiement est facturé sur votre compte AWS dans les 12 heures qui suivent l'achat d'un bloc de capacité. Pendant le traitement de votre

paiement, votre ressource de réservation de bloc de capacité reste en état d'`payment-pending`. Si votre paiement ne peut pas être traité dans un délai de 12 heures, votre bloc de capacité est libéré et l'état de la réservation passe à `payment-failed`.

Une fois votre paiement traité avec succès, l'état de la ressource de bloc de capacité passe de `payment-pending` à `scheduled`. Vous recevez une facture qui reflète le paiement initial unique. Dans la facture, vous pouvez associer le montant payé à l'identifiant de réservation de bloc de capacité.

Lorsque votre réservation de bloc de capacité commence, vous êtes facturé uniquement en fonction du système d'exploitation que vous utilisez pendant que vos instances sont exécutées dans le cadre de la réservation. Vous pouvez consulter votre utilisation et les frais associés sur votre facture anniversaire pour le mois d'utilisation de votre AWS Cost and Usage Report.

Note

Les remises sur les Savings Plans et les instances réservées ne s'appliquent pas aux blocs de capacité.

Affichage d'une facture

Vous pouvez consulter votre facture dans la AWS Billing and Cost Management console. Le paiement initial de votre bloc de capacité apparaît le mois au cours duquel vous avez acheté la réservation.

Après le début de votre réservation, votre facture indique des lignes distinctes pour le temps de réservation du bloc utilisé et le temps non utilisé. Vous pouvez utiliser ces lignes pour voir combien de temps a été utilisé pour votre réservation. Vous ne verrez des frais d'utilisation dans la ligne correspondant au temps utilisé que si vous utilisez un système d'exploitation premium. Pour plus d'informations, consultez [Tarification](#). Le temps non utilisé n'entraîne aucun frais supplémentaires.

Pour plus d'informations, consultez la section [Viewing your bill](#) (Affichage d'une facture) dans le Guide de l'utilisateur AWS Billing and Cost Management .

Si votre bloc de capacité commence à un mois différent de celui au cours duquel vous avez acheté votre réservation, le prix initial et l'utilisation de la réservation apparaissent sous des mois de facturation distincts. Dans votre AWS Cost and Usage Report, le numéro de réservation Capacity Block est indiqué dans la rubrique Reservation/ReservationArn de vos frais initiaux et dans le

LinItem/ResourceID de votre facture anniversaire afin que vous puissiez associer l'utilisation au prix initial correspondant.

Utiliser des blocs de capacité

Pour commencer à utiliser les blocs de capacité, vous devez d'abord rechercher et acheter un bloc de capacité disponible qui correspond à la taille, à la durée et au calendrier de votre réservation. Ensuite, lorsque la réservation commence, vous pouvez utiliser le bloc de capacité en lançant des instances qui ciblent l'ID de réservation. Trente minutes avant l'expiration de la réservation, nous commençons à mettre fin à toutes les instances encore en cours d'exécution dans le bloc de capacité.

Les blocs de capacité sont fournis sous forme de réserve de capacité `targeted` dans une seule zone de disponibilité. Pour exécuter des instances dans un bloc de capacité, vous devez spécifier l'ID de réservation lors du lancement de vos instances. Si vous arrêtez vous-même des instances et que le bloc de capacité expire, vous ne pouvez pas les redémarrer tant que vous n'avez pas ciblé un autre bloc de capacité à l'état `active`.

Par défaut, les blocs de capacité fournissent une connectivité réseau à faible latence et à haut débit entre les instances du bloc de capacité. Il n'est donc pas nécessaire d'utiliser un groupe de placement du cluster avec un bloc de capacité.

Rubriques

- [Prérequis](#)
- [Rechercher et acheter des blocs de capacité](#)
- [Lancer des instances dans des blocs de capacité](#)
- [Afficher les blocs de capacité](#)

Prérequis

Vous devez utiliser la Région AWS correspondant au type d'instance que vous souhaitez utiliser. Pour plus d'informations, consultez [Régions](#).

Les blocs de capacité avec `p5.48xlarge` instances sont disponibles ci-dessous Régions AWS.

Nom de la région	Code région
USA Est (Ohio)	us-east-2

Nom de la région	Code région
USA Est (Virginie du Nord)	us-east-1

Les blocs de capacité avec p4d.24xlarge instances sont disponibles ci-dessous Régions AWS.

Nom de la région	Code région
USA Est (Ohio)	us-east-2
USA Ouest (Oregon)	us-west-2

Note

Les tailles de bloc de capacité de 64 instances ne sont pas prises en charge pour tous les types d'instances Régions AWS.

Rechercher et acheter des blocs de capacité

Pour réserver un bloc de capacité, vous devez d'abord rechercher un intervalle de temps pendant lequel la capacité est disponible et qui correspond à vos besoins. Pour trouver un bloc de capacité disponible à la réservation, vous devez spécifier ce qui suit.

- Le nombre d'instances dont vous avez besoin
- La durée pendant laquelle vous avez besoin des instances
- La plage de dates pour laquelle vous avez besoin de votre réservation

Pour rechercher une offre de bloc de capacité disponible, vous devez spécifier une durée de réservation et un nombre d'instances. Vous devez sélectionner l'une des options suivantes.

- Pour la durée de la réservation : jusqu'à 14 jours par incrément d'un jour
- Par nombre d'instances : 1, 2, 4, 8, 16, 32 ou 64 instances

Si un bloc de capacité correspondant à vos spécifications est disponible, nous vous renvoyons les détails d'une seule offre de bloc de capacité. Les détails de l'offre incluent l'heure de début

de la réservation, la zone de disponibilité de la réservation et le prix de la réservation. Pour plus d'informations, consultez [Tarification](#).

Vous pouvez acheter l'offre de bloc de capacité qui vous est présentée, ou vous pouvez modifier vos critères de recherche pour voir les autres options disponibles. Il n'y a pas de date d'expiration prédéfinie pour l'offre, mais les offres sont disponibles uniquement sur le principe du premier arrivé, premier servi.

Lorsque vous achetez une offre de bloc de capacité, vous recevez une réponse immédiate confirmant que votre bloc de capacité a été réservé. Après confirmation, vous verrez une nouvelle réserve de capacité sur votre compte avec un type de réservation `capacity-block` et une `start-date` définie pour l'offre que vous avez achetée. Votre réservation de bloc de capacité est créée avec l'état `payment-pending`. Une fois le paiement initial traité avec succès, l'état de la réservation passe à `scheduled`. Pour plus d'informations, consultez [Facturation](#).

Vous pouvez utiliser l'une des méthodes suivantes pour rechercher et acheter un bloc de capacité.

Console

Pour rechercher et acheter un bloc de capacité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation en haut de l'écran, sélectionnez un Région AWS. Ce choix est important car les tailles de blocs de capacité de 64 instances ne sont pas prises en charge pour tous les types d'instances dans toutes les régions.
3. Dans le volet de navigation, choisissez Réserve de capacité, Acheter des blocs de capacité.
4. Sous Attributs de capacité, vous pouvez définir les paramètres de recherche de votre bloc de capacité. Par défaut, la plateforme est Linux. Si vous souhaitez sélectionner un autre système d'exploitation, utilisez l' AWS CLI. Pour plus d'informations, consultez [Plateformes prises en charge](#).
5. Sous Capacité totale, sélectionnez le nombre d'instances que vous souhaitez réserver.
6. Sous Durée, saisissez le nombre de jours pour lesquels vous avez besoin de la réservation.
7. Sous Plage de dates pour rechercher des blocs de capacité, saisissez la date de début la plus proche possible et la dernière date de fin acceptable pour votre réservation.
8. Choisissez Rechercher des blocs de capacité.
9. Si un bloc de capacité répondant à vos spécifications est disponible, une offre s'affiche sous Blocs de capacité recommandés. Si plusieurs offres répondent à vos spécifications, l'offre de

bloc de capacité la moins chère disponible s'affiche. Pour consulter les autres offres de blocs de capacité, ajustez vos critères de recherche et sélectionnez à nouveau Rechercher des blocs de capacité.

10. Lorsque vous trouvez une offre de bloc de capacité que vous souhaitez acheter, choisissez Suivant.
11. (Facultatif) Sur la page Ajouter des balises, choisissez Ajouter une nouvelle balise.
12. La page Vérifier et acheter répertorie les dates de début et de fin, la durée, le nombre total d'instances et le prix.

Note

Les blocs de capacité ne peuvent être ni modifiés ni annulés une fois que vous les avez réservés.

13. Dans la fenêtre contextuelle Acheter un bloc de capacité, saisissez « confirm », puis choisissez Acheter.

AWS CLI

Pour trouver un bloc de capacité à l'aide du AWS CLI

Utilisez la commande `describe-capacity-block-offerings`.

L'exemple suivant recherche un bloc de capacité comportant 16 instances `p5.48xlarge`, dont la plage de dates commence le `2023-08-14` et se termine le `2023-10-22` avec une durée de 48 heures. Le nombre d'instances doit être un entier provenant d'un ensemble prédéfini d'options 1, 2, 4, 8, 16, 32 ou 64. La durée de la capacité doit être un entier multiple de 24 compris entre 24 et 336 indiquant le nombre de jours en heures.

```
aws ec2 describe-capacity-block-offerings --instance-type p5.48xlarge \  
--instance-count 16 --start-date-range 2023-08-14T00:00:00Z \  
--end-date-range 2023-10-22-T00:00:00Z --capacity-duration 48
```

Pour acheter un bloc de capacité à l'aide du AWS CLI

Utilisez la commande `purchase-capacity-block` et spécifiez l'ID de l'offre de bloc de capacité que vous souhaitez acheter et la plateforme de l'instance.

```
aws ec2 purchase-capacity-block \  
  --capacity-block-offering-id cbr-0123456789abcdefg \  
  --instance-platform Linux/UNIX
```

Lancer des instances dans des blocs de capacité

Après avoir réservé un bloc de capacité, vous pouvez consulter la réservation du bloc de capacité dans votre compte AWS . Vous pouvez consulter la `start-date` et la `end-date` pour savoir quand votre réservation débute et se termine. Avant le début d'une réservation de bloc de capacité, la capacité disponible apparaît comme nulle. Vous pouvez voir combien d'instances seront disponibles dans votre bloc de capacité en fonction de la valeur de balise associée à la clé de balise `aws:ec2capacityreservation:incrementalRequestedQuantity`.

Lorsqu'une réservation de bloc de capacité commence, l'état de la réservation passe de `scheduled` à `active`. Nous émettons un événement via Amazon EventBridge pour vous informer que le Capacity Block est prêt à être utilisé. Pour plus d'informations, consultez [Surveiller les blocs de capacité](#).

Pour utiliser votre bloc de capacité, vous devez spécifier l'ID de réservation de bloc de capacité lors du lancement des instances. Le lancement d'une instance dans un bloc de capacité réduit la capacité disponible du nombre d'instances lancées. Par exemple, si la capacité d'instance que vous avez achetée est de huit instances et que vous lancez quatre instances, la capacité disponible est réduite de quatre.

Si vous mettez fin à une instance exécutée dans le bloc de capacité avant la fin de la réservation, vous pouvez lancer une nouvelle instance à sa place. Lorsque vous arrêtez ou mettez fin à une instance dans un bloc de capacité, le nettoyage de votre instance prend plusieurs minutes avant de pouvoir lancer une autre instance pour la remplacer. Pendant ce temps, votre instance sera à l'état `Arrêt` ou `shutting-down`. Une fois ce processus terminé, l'état de votre instance deviendra `stopped` ou `terminated`. Ensuite, la capacité disponible dans votre bloc de capacité sera mise à jour pour afficher une autre instance disponible à utiliser.

Les étapes suivantes expliquent comment lancer des instances dans un bloc de capacité à `active` l'aide du AWS Management Console ou du AWS CLI.

Pour plus d'informations sur la configuration d'un groupe de nœuds EKS pour utiliser automatiquement un bloc de capacité lorsqu'il commence, consultez la rubrique [Blocs de capacité pour ML](#) (français non garanti) dans le Guide de l'utilisateur Amazon EKS.

Pour plus d'informations sur le lancement d'instances dans un bloc de capacité à l'aide de la flotte d'EC2, consultez la rubrique [Tutoriel : Lancer des instances dans des blocs de capacité](#).

Pour plus d'informations sur la création d'un modèle de lancement ciblant un bloc de capacité, consultez la rubrique [Lancer une instance à partir d'un modèle de lancement](#).

Vous pouvez utiliser l'une des méthodes suivantes pour lancer des instances dans un bloc de capacité.

Console

Pour lancer des instances dans un bloc de capacité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, en haut de l'écran, sélectionnez la région de votre réservation de bloc de capacité.
3. Sur le tableau de bord de la console Amazon EC2, sélectionnez Launch instance (Lancer une instance).
4. (Facultatif) Sous Nom et balises, vous pouvez nommer et baliser votre instance. Pour plus d'informations sur les balises, consultez [Baliser vos ressources Amazon EC2](#)
5. Sous Images d'applications et de systèmes d'exploitation, sélectionnez une Amazon Machine Image (AMI).
6. Sous Type d'instance, sélectionnez le type d'instance qui correspond à votre réservation de bloc de capacité.
7. Sous Paire de clés (connexion), choisissez une paire de clés existante ou choisissez Créer une paire de clés pour en créer une. Pour plus d'informations, consultez [Paires de clés Amazon EC2 et instances Amazon EC2](#).
8. Sous Network settings (Paramètres réseau), utilisez les paramètres par défaut ou choisissez Edit (Modifier) pour configurer les paramètres réseau selon les besoins.

Important

Votre instance ne peut pas être lancée dans un sous-réseau situé dans une zone de disponibilité différente de celle dans laquelle se trouve votre bloc de capacité.

9. Sous Détails avancés, configurez l'instance Spot comme suit.
 - a. Sous Option d'achat (type de marché), sélectionnez Bloc de capacité.

- b. Sous Réserve de capacité, sélectionnez Cible par ID.
 - c. Sélectionnez l'ID de réserve de capacité de votre réservation de bloc de capacité.
10. Sur le panneau Summary (Récapitulatif), pour Number of instances (Nombre d'instances), saisissez le nombre d'instances à lancer.
 11. Choisissez Launch instance (Lancer une instance).

AWS CLI

Pour lancer des instances dans un bloc de capacité à l'aide du AWS CLI

- Utilisez la commande `run-instances` et spécifiez un `MarketType` de `capacity-block` dans la structure `instance-market-options`. Vous devez également spécifier le paramètre `capacity-reservation-specification`.

L'exemple suivant lance une instance `p5.48xlarge` unique dans un bloc de capacité actif disposant des attributs correspondants et de la capacité disponible.

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 \  
  --instance-type p5.48xlarge --key-name MyKeyPair \  
  --subnet-id subnet-1234567890abcdef1 \  
  --instance-market-options MarketType='capacity-block' \  
  --capacity-reservation-specification \  
  CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

Afficher les blocs de capacité

Les états des blocs de capacité sont les suivants :

- `payment-pending` : le paiement initial n'a pas encore été traité.
- `payment-failed` : le paiement n'a pas pu être traité dans un délai prévu des 12 heures. Votre bloc de capacité a été libéré.
- `scheduled` : le paiement a été traité et la réservation du bloc de capacité n'a pas encore commencé.
- `active` : la capacité réservée peut être utilisée.
- `expired` : la réservation de bloc de capacité a expiré automatiquement à la date et à l'heure spécifiées dans votre demande de réservation. La capacité réservée n'est plus disponible pour utilisation.

Vous pouvez utiliser l'une des méthodes ci-dessous pour afficher votre réservation de bloc de capacité.

Console

Pour afficher les blocs de capacité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Réservations de capacité.
3. Sur la page Aperçu des réservations de capacité, vous pouvez voir un table des ressources contenant des détails sur toutes vos ressources de réserve de capacité. Pour trouver vos réservations de blocs de capacité, sélectionnez les blocs de capacité dans la liste déroulante située au-dessus de l'ID de réserve de capacité. Dans la table, vous pouvez consulter des informations sur vos blocs de capacité, telles que les dates de début et de fin, la durée et le statut.
4. Pour plus de détails sur un bloc de capacité, sélectionnez l'ID de réservation de bloc de capacité que vous souhaitez consulter. La page Détails de réserve de capacité affiche toutes les propriétés de la réservation ainsi que le nombre d'instances utilisées et disponibles dans le bloc de capacité.

Note

Avant le début d'une réservation de bloc de capacité, la capacité disponible apparaît comme nulle. Vous pouvez voir combien d'instances seront disponibles lorsque la réservation du bloc de capacité commence à l'aide de la valeur de balise suivante associée à la clé de balise :
`aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

Pour afficher les blocs de capacité à l'aide du AWS CLI

Par défaut, lorsque vous utilisez la commande [describe-capacity-reservations](#), les réserves de capacité à la demande et les réservations par blocs de capacité sont répertoriées. Pour afficher uniquement vos réservations de blocs de capacité, filtrez le paramètre `capacity-reservation-type` à l'aide de `capacity-block`.

Par exemple, la commande suivante décrit une ou plusieurs de vos réservations Capacity Block dans votre compte actuel Région AWS.

```
aws ec2 describe-capacity-reservations --reservation-type capacity-block
```

Exemple de sortie.

```
{
  "CapacityReservations": [
    {
      "CapacityReservationId": "cr-12345678",
      "EndDateType": "limited",
      "ReservationType": "capacity-block",
      "AvailabilityZone": "eu-east-2a",
      "InstanceMatchCriteria": "targeted",
      "EphemeralStorage": false,
      "CreateDate": "2023-11-29T14:22:45Z",
      "StartDate": "2023-12-15T12:00:00Z",
      "EndDate": "2023-08-19T12:00:00Z",
      "AvailableInstanceCount": 0,
      "InstancePlatform": "Linux/UNIX",
      "TotalInstanceCount": 16,
      "State": "payment-pending",
      "Tenancy": "default",
      "EbsOptimized": true,
      "InstanceType": "p5.48xlarge"
    },
    ...
  ]
}
```

Surveiller les blocs de capacité

Rubriques

- [Surveillez les blocs de capacité avec EventBridge](#)
- [La capacité de journalisation bloque les appels d'API avec AWS CloudTrail](#)

Surveillez les blocs de capacité avec EventBridge

Lorsque votre réservation de bloc de capacité commence, Amazon EC2 émet un événement indiquant EventBridge que votre capacité est prête à être utilisée. Quarante minutes avant la fin de

vosre réservation Capacity Block, vous recevez un autre EventBridge événement vous indiquant que toutes les instances incluses dans la réservation commenceront à se terminer dans 10 minutes. Pour plus d'informations sur EventBridge les événements, consultez [Amazon EventBridge Events](#).

Les structures d'événements suivantes pour les événements émis pour les blocs de capacité :

Bloc de capacité remis

L'exemple suivant présente un événement pour un bloc de capacité remis.

```
{
  "customer_event_id": "[Capacity Reservation Id]-delivered",
  "detail_type": "Capacity Block Reservation Delivered",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Avertissement d'expiration du bloc de capacité

L'exemple suivant présente un événement pour un avertissement d'expiration d'un bloc de capacité.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Reservation Expiration Warning",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

}

La capacité de journalisation bloque les appels d'API avec AWS CloudTrail

Capacity Blocks est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Capacity Blocks. CloudTrail capture les appels d'API pour les blocs de capacité sous forme d'événements. Ces appels capturés incluent les appels de la console des blocs de capacité et les appels de code vers les opérations de l'API des blocs de capacité. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour les blocs de capacité. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Capacity Blocks, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Informations sur les blocs de capacité dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans des blocs de capacité, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements qui se produisent dans votre environnement Compte AWS, y compris les événements liés aux blocs de capacité, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- [Présentation de la création d'un journal de suivi](#)
- [CloudTrail services et intégrations pris en charge](#)

- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Toutes les actions des Capacity Blocks sont enregistrées CloudTrail et documentées dans le manuel Amazon EC2 API Reference. Par exemple, les appels au `CapacityBlockScheduled` et les `CapacityBlockActive` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément [CloudTrail UserIdentity](#).

Présentation des entrées des fichiers journaux des blocs de capacité

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Les exemples suivants montrent les entrées du CloudTrail journal pour :

- [TerminateCapacityBlocksInstances](#)
- [CapacityBlockPaymentFailed](#)
- [CapacityBlockProgrammé](#)
- [CapacityBlockActif](#)
- [CapacityBlockÉchoué](#)

- [CapacityBlockExpiré](#)

Note

Certains champs qui ont été supprimés des exemples relatifs à la confidentialité des données.

TerminateCapacityBlocksInstances

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 boto3/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:instance/i-1234567890abcdef0"
    },
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws::ec2:US East (N. Virginia):123456789012:instance/i-0598c7d356eba48d7"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
}
```

```
"serviceEventDetails": {
  "capacityReservationId": "cr-12345678",
}
}
```

CapacityBlockPaymentFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 boto3/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
    "capacityReservationId": "cr-12345678",
    "capacityReservationState": "payment-failed"
  }
}
```

CapacityBlockProgrammé

```
{
  "eventVersion": "1.05",
```

```
"userIdentity": {
  "accountId": "123456789012",
  "invokedBy": "AWS Internal;"
},
"eventTime": "2023-10-02T00:06:08Z",
"eventSource": "ec2.amazonaws.com",
"eventName": "CapacityBlockScheduled",
"awsRegion": "us-east-1",
"sourceIPAddress": "203.0.113.25",
"userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
"requestParameters": null,
"responseElements": null,
"eventID": "a1b2c3d4-EXAMPLE",
"readOnly": false,
"resources": [
  {
    "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
    "accountId": "123456789012",
    "type": "AWS::EC2::CapacityReservation"
  }
],
"eventType": "AwsServiceEvent",
"recipientAccountId": "123456789012",
"serviceEventDetails": {
  "capacityReservationId": "cr-12345678",
  "capacityReservationState": "scheduled"
}
}
```

CapacityBlockActif

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
```

```

"userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
"requestParameters": null,
"responseElements": null,
"eventID": "a1b2c3d4-EXAMPLE",
"readOnly": false,
"resources": [
  {
    "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
    "accountId": "123456789012",
    "type": "AWS::EC2::CapacityReservation"
  }
],
"eventType": "AwsServiceEvent",
"recipientAccountId": "123456789012",
"serviceEventDetails": {
  "capacityReservationId": "cr-12345678",
  "capacityReservationState": "active"
}
}

```

CapacityBlockÉchoué

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",

```

```

    "accountId": "123456789012",
    "type": "AWS::EC2::CapacityReservation"
  }
],
"eventType": "AwsServiceEvent",
"recipientAccountId": "123456789012",
"serviceEventDetails": {
  "capacityReservationId": "cr-12345678",
  "capacityReservationState": "failed"
}
}

```

CapacityBlockExpiré

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
    "capacityReservationId": "cr-12345678",
    "capacityReservationState": "expired"
  }
}

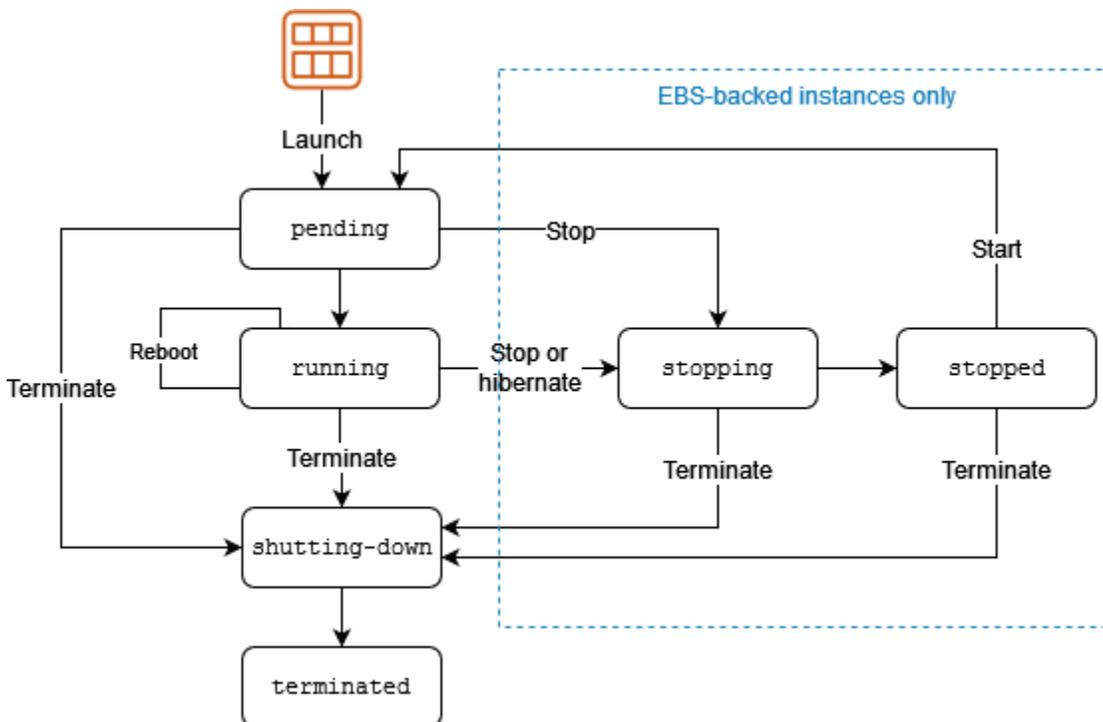
```

```
}
}
```

Cycle de vie d'une instance

Une instance Amazon EC2 passe par différents états entre le moment où vous la lancez et où vous la désactivez.

L'illustration suivante représente les transitions entre les états de l'instance. Notez que vous ne pouvez pas arrêter et démarrer une instance basée sur le stockage d'instances. Pour plus d'informations sur les instances basées sur le stockage d'instances, consultez [Stockage pour le périphérique racine](#).



Le tableau suivant fournit une brève description de l'état de chaque instance et indique si l'utilisation de l'instance est facturée. Certaines AWS ressources, telles que les volumes Amazon EBS et les adresses IP Elastic, sont facturées quel que soit l'état de l'instance. Pour plus d'informations, consultez [Éviter les frais inattendus](#) dans le Guide de l'utilisateur AWS Billing .

État de l'instance	Description	Facturation de l'utilisation de l'instance
pending	L'instance se prépare à passer à l'état <code>running</code> . Une instance passe à l'état <code>pending</code> lorsqu'elle est lancée ou lorsqu'elle est démarrée après avoir été à l'état <code>stopped</code> .	Non facturé
running	L'instance est en cours d'exécution et prête à être utilisée.	Facturé
stopping	L'instance se prépare à être arrêtée.	Non facturé
stopped	L'instance est arrêtée et ne peut pas être utilisée. L'instance peut être démarrée à tout moment.	Non facturé
shutting down	L'instance se prépare à être supprimée.	Non facturé
terminated	L'instance a été définitivement supprimée et ne peut pas être démarrée.	Non facturé

 **Note**

Les instances réservées appliquées aux instances résiliées sont facturées jusqu'à la fin de leur période de validité, selon l'option de paiement. Pour plus d'informations, consultez [Reserved instances](#).

Table des matières

- [Lancement d'une instance](#)
- [Arrêt et démarrage d'une instance \(instances basées sur les volumes Amazon EBS uniquement\)](#)
- [Mise en veille prolongée d'une instance \(instances basées sur Amazon EBS uniquement\)](#)
- [Redémarrage d'instance](#)
- [Terminaison d'instance](#)
- [Différences entre redémarrage, arrêt, mise en veille prolongée et résiliation](#)
- [Lancer votre instance](#)
- [Arrêtez et démarrez les instances Amazon EC2](#)
- [Hibernez votre instance Amazon EC2](#)
- [Redémarrer votre instance](#)
- [Mettre fin aux instances Amazon EC2](#)
- [Mise hors service d'instance](#)
- [Résilience de l'instance](#)

Lancement d'une instance

Lorsque vous lancez une instance, elle entre dans l'état `pending`. Le type d'instance que vous avez spécifié au lancement détermine les capacités matérielles de l'ordinateur hôte de votre instance. Nous utilisons l'Amazon Machine Image (AMI) que vous avez spécifié au lancement pour démarrer l'instance. Une fois que l'instance est prête, elle entre dans l'état `running`. Vous pouvez vous connecter à votre instance en cours d'exécution et l'utiliser comme vous le feriez d'un ordinateur devant lequel vous êtes assis.

Dès que votre instance passe à l'état `running`, vous êtes facturé pour chaque seconde d'exécution de l'instance, avec un minimum d'une minute, même si l'instance demeure inactive et que vous ne vous y connectez pas.

Arrêt et démarrage d'une instance (instances basées sur les volumes Amazon EBS uniquement)

Si votre instance ne passe pas avec succès un contrôle de statut ou n'exécute pas vos applications comme escompté, et que le volume racine de votre instance est un volume Amazon EBS, vous pouvez arrêter et démarrer votre instance pour tenter de corriger le problème.

Lorsque vous arrêtez votre instance, elle entre dans l'état `stopping`, puis dans l'état `stopped`. Aucuns frais d'utilisation ou de transfert de données ne vous sont facturés pour votre instance lorsqu'elle est `stopped`. Des frais sont facturés pour le stockage de tous les volumes Amazon EBS. Lorsque votre instance se trouve dans l'état `stopped`, vous pouvez modifier certains attributs de l'instance, y compris le type d'instance.

Lorsque vous démarrez votre instance, elle passe à l'état `pending` et elle est déplacée vers un nouvel ordinateur hôte (même si, dans la plupart des cas, elle reste sur l'hôte actuel). Lorsque vous arrêtez et démarrez votre instance, vous perdez toutes les données des volumes de stockage d'instances attachés à l'ordinateur hôte précédent.

Votre instance conserve son adresse IPv4 privée, ce qui signifie qu'une adresse IP Elastic associée à l'adresse IPv4 privée ou à l'interface réseau reste associée à votre instance. Si votre instance a une adresse IPv6, elle conserve l'adresse IPv6.

Chaque fois que vous opérez la transition d'une instance de l'état `stopped` à l'état `running`, vous êtes facturé par seconde d'exécution de l'instance, avec un minimum d'une minute par instance démarrée.

Pour plus d'informations sur l'arrêt et le redémarrage d'une instance, consultez [Arrêtez et démarrez les instances Amazon EC2](#).

Mise en veille prolongée d'une instance (instances basées sur Amazon EBS uniquement)

Lorsque vous mettez une instance en veille prolongée, nous demandons au système d'exploitation d'exécuter l'opération correspondante (`suspend-to-disk`), ce qui enregistre le contenu de la mémoire de l'instance (RAM) sur votre volume racine Amazon EBS. Nous conservons le volume racine Amazon EBS de l'instance et les volumes de données Amazon EBS attachés. Lorsque vous démarrez votre instance, le volume racine Amazon EBS est restauré à son état précédent et le contenu de la mémoire RAM est rechargé. Les volumes de données précédemment attachés sont attachés à nouveau et l'instance conserve son ID d'instance.

Lorsque vous mettez votre instance en veille prolongée, elle entre dans l'état `stopping`, puis dans l'état `stopped`. Nous ne facturons pas l'utilisation d'une instance en veille prolongée à l'état `stopped`, mais nous la facturons quand elle est à l'état `stopping`, contrairement à ce qui se produit quand vous [arrêtez une instance](#) sans la mettre en veille prolongée. Nous ne facturons pas de frais de transfert de données pour l'utilisation. En revanche, nous facturons le stockage des volumes Amazon EBS, y compris le stockage des données de la mémoire RAM.

Lorsque vous démarrez votre instance mise en veille prolongée, elle passe à l'état `pending` et nous déplaçons l'instance vers un nouvel ordinateur hôte (même si, dans la plupart des cas, elle reste sur l'hôte actuel).

Votre instance conserve son adresse IPv4 privée, ce qui signifie qu'une adresse IP Elastic associée à l'adresse IPv4 privée ou à l'interface réseau continue d'être associée à votre instance. Si votre instance a une adresse IPv6, elle conserve cette dernière.

Pour plus d'informations, consultez [Hibernez votre instance Amazon EC2](#).

Redémarrage d'instance

Vous pouvez redémarrer votre instance à l'aide de la console Amazon EC2, d'un outil de ligne de commande et de l'API Amazon EC2. Nous vous recommandons d'utiliser Amazon EC2 pour redémarrer votre instance au lieu d'exécuter la commande de redémarrage du système d'exploitation à partir de votre instance.

Le redémarrage d'une instance est similaire à celui d'un système d'exploitation. L'instance demeure sur le même ordinateur hôte et conserve son nom DNS public, son adresse IP privée et les données de ses volumes de stockage d'instances. Le redémarrage nécessite généralement quelques minutes pour s'exécuter, mais le temps réel dépend de la configuration de l'instance.

Le redémarrage d'une instance ne déclenche pas de nouvelle période de facturation ; la facturation par seconde se poursuit, sans frais minimum d'une minute.

Pour plus d'informations, consultez [Redémarrer votre instance](#).

Terminaison d'instance

Si vous jugez que vous n'avez plus besoin d'une instance, vous pouvez la mettre hors service. Dès que l'état d'une instance passe à `shutting-down` ou `terminated`, l'instance ne vous est plus facturée.

Si vous activez la protection de la résiliation, il ne vous est pas possible de résilier l'instance à l'aide de la console, de la CLI ou de l'API.

Une fois que vous avez mis une instance hors service, elle demeure visible sur la console pendant un court instant, puis l'entrée est supprimée automatiquement. Vous pouvez aussi décrire une instance terminée à l'aide de la CLI ou de l'API. Les ressources (telles que les balises) sont progressivement dissociées de l'instance résiliées. Par conséquent, elles ne seront plus visibles dans l'instance

terminée après un certain temps. Vous ne pouvez pas vous connecter à une instance terminée, ni la récupérer.

Chaque instance basée sur Amazon EBS prend en charge

l'attribut `InstanceInitiatedShutdownBehavior`, qui contrôle si l'instance s'arrête ou se termine lorsque vous lancez l'arrêt depuis l'instance elle-même (par exemple, en utilisant la `shutdown` commande sous Linux). Le comportement par défaut est celui de l'arrêt de l'instance. Vous pouvez modifier la valeur de cet attribut tandis que l'instance est en cours d'exécution ou arrêtée.

Chaque volume Amazon EBS prend en charge l'attribut `DeleteOnTermination`, qui contrôle si le volume est supprimé ou conservé lorsque vous terminez l'instance à laquelle il est attaché. Par défaut, le volume du périphérique racine est supprimé et les autres volumes EBS sont conservés.

Pour plus d'informations, consultez [Mettre fin aux instances Amazon EC2](#).

Différences entre redémarrage, arrêt, mise en veille prolongée et résiliation

Le tableau suivant résume les principales différences entre le redémarrage, l'arrêt, la mise en veille prolongée et la résiliation d'une instance.

Caractéristiques	Redémarrer	Arrêt/démarrage (instances basées sur les volumes Amazon EBS uniquement)	Mise en veille prolongée (instances basées sur Amazon EBS uniquement)	Terminer
Ordinateur hôte	L'instance demeure sur le même ordinateur hôte.	Nous déplaçons l'instance vers un nouvel ordinateur hôte (même si, dans certains cas, elle reste sur l'hôte actuel).	Nous déplaçons l'instance vers un nouvel ordinateur hôte (même si, dans certains cas, elle reste sur l'hôte actuel).	Aucun
Adresses IP publiques et privées	Ces adresses demeurent identiques.	L'instance conserve son adresse IPv4 privée. L'instance obtient une nouvelle adresse IPv4	L'instance conserve son adresse IPv4 privée. L'instance obtient une nouvelle adresse IPv4	Aucun

Caractéristiques	Redémarrer	Arrêt/démarrage (instances basées sur les volumes Amazon EBS uniquement)	Mise en veille prolongée (instances basées sur Amazon EBS uniquement)	Terminer
		publique, à moins qu'elle ne possède une adresse IP Elastic, laquelle ne change pas lors d'un arrêt/démarrage.	publique, à moins qu'elle ne possède une adresse IP Elastic, laquelle ne change pas lors d'un arrêt/démarrage.	
Adresses IP Elastic (IPv4)	L'adresse IP Elastic reste associée à l'instance	L'adresse IP Elastic reste associée à l'instance	L'adresse IP Elastic reste associée à l'instance	L'adresse IP Elastic est dissociée de l'instance.
Adresse IPv6	L'instance conserve son adresse IPv6.	L'instance conserve son adresse IPv6.	L'instance conserve son adresse IPv6.	Aucun
Volumes de stockage d'instances	Les données sont conservées.	Les données sont effacées.	Les données sont effacées.	Les données sont effacées.
volume du périphérique racine	Le volume est conservé	Le volume est conservé	Le volume est conservé	Le volume est supprimé par défaut.
RAM (contenu de la mémoire)	Les données de la mémoire RAM sont effacées.	Les données de la mémoire RAM sont effacées.	La mémoire RAM est enregistrée dans un fichier sur le volume racine.	Les données de la mémoire RAM sont effacées.

Caractéristiques	Redémarrer	Arrêt/démarrage (instances basées sur les volumes Amazon EBS uniquement)	Mise en veille prolongée (instances basées sur Amazon EBS uniquement)	Terminer
Facturation	L'heure de facturation de l'instance ne change pas	Vous cessez d'être facturé aussitôt que l'état d'une instance devient <code>stopping</code> . Chaque fois qu'une instance passe de l'état <code>stopped</code> à l'état <code>running</code> , nous commençons une nouvelle période de facturation, en facturant un minimum d'une minute à chaque démarrage de l'instance.	Des frais vous sont facturés lorsque l'instance est à l'état <code>stopping</code> , mais ne le sont plus lorsque l'instance passe à l'état <code>stopped</code> . Chaque fois qu'une instance passe de l'état <code>stopped</code> à l'état <code>running</code> , nous commençons une nouvelle période de facturation, en facturant un minimum d'une minute à chaque démarrage de l'instance.	Vous arrêtez de payer des frais pour une instance dès que son état passe à <code>shutting-down</code>

Les commandes d'arrêt du système d'exploitation terminent toujours une instance basée sur le stockage d'instances. Vous pouvez contrôler si les commandes d'arrêt du système d'exploitation arrêtent ou terminent une instance basée sur les volumes Amazon EBS. Pour plus d'informations, consultez [Modifier le comportement d'arrêt lancé de l'instance](#).

Lancer votre instance

Une instance est un serveur virtuel dans le AWS Cloud. Vous lancez une instance à partir d'une Amazon Machine Image (AMI). L'AMI fournit le système d'exploitation, le serveur d'applications, ainsi que les applications de votre instance.

Lorsque vous vous inscrivez AWS, vous pouvez commencer à utiliser Amazon EC2 gratuitement en utilisant le niveau [AWS gratuit](#). Vous pouvez utiliser l'offre gratuite pour lancer et utiliser une instance `t2.micro` gratuitement pendant 12 mois (dans les régions où `t2.micro` n'est pas disponible, vous pouvez utiliser une instance `t3.micro` avec l'offre gratuite). Si vous lancez une instance qui ne fait pas partie de l'offre gratuite, les frais d'utilisation standard d'Amazon EC2 vous seront facturés pour l'instance. Pour plus d'informations, consultez [Tarification Amazon EC2](#).

Vous pouvez lancer une instance à l'aide des méthodes suivantes.

Méthode	Documentation
[Console Amazon EC2] Utilisation de l'assistant de lancement d'instance pour spécifier les paramètres de lancement.	Lancer une instance à l'aide de l'ancien assistant de lancement d'instance
[Console Amazon EC2] Création d'un modèle de lancement et lancement de l'instance à partir de celui-ci.	Lancer une instance à partir d'un modèle de lancement
[Console Amazon EC2] Utilisation d'une instance existante comme base.	Lancer une instance à l'aide des paramètres d'une instance existante
[Console Amazon EC2] Utilisez une AMI que vous avez achetée sur AWS Marketplace.	Lancer une AWS Marketplace instance
[AWS CLI] Utilisation d'une AMI que vous sélectionnez.	Utilisation d'Amazon EC2 via la CLI AWS
[AWS Tools for Windows PowerShell] Utilisation d'une AMI que vous sélectionnez.	Amazon EC2 à partir du AWS Tools for Windows PowerShell
[AWS CLI] Utilisez la flotte EC2 pour allouer la capacité entre différents types d'instance EC2 et zones de disponibilité, et entre les modèles d'achat d'instance à la demande, d'instance réservée et d'instance Spot.	EC2 Fleet

Méthode	Documentation
[AWS CloudFormation] Utilisez un AWS CloudFormation modèle pour spécifier une instance.	AWS::EC2::Instance dans le guide de l'utilisateur AWS CloudFormation
[AWS SDK] Utilisez un AWS SDK spécifique au langage pour lancer une instance.	AWS SDK pour .NET AWS SDK pour C++ AWS SDK pour Go AWS SDK pour Java AWS SDK pour JavaScript AWS SDK pour PHP V3 AWS SDK pour Python AWS SDK pour Ruby V3

 Note

Pour lancer une instance EC2 dans un sous-réseau IPv6 uniquement, vous devez utiliser des [instances basées](#) sur le système Nitro. AWS

 Note

Lors du lancement d'une instance IPv6 uniquement, il est possible que DHCPv6 ne fournisse pas immédiatement à l'instance le serveur de noms DNS IPv6. Au cours de ce délai initial, l'instance peut ne pas être en mesure de résoudre les domaines publics.

Pour les instances exécutées sur Amazon Linux 2, si vous souhaitez mettre immédiatement à jour le fichier `/etc/resolv.conf` avec le serveur de noms DNS IPv6, exécutez la commande `cloud-init` directive suivante lors du lancement :

```
#cloud-config
bootcmd:
```

```
- /usr/bin/sed -i -E 's,^nameserver\s+[\.[:digit:]]+$/,nameserver
fd00:ec2::253,' /etc/resolv.conf
```

Une autre option consiste à modifier le fichier de configuration et à recréer une image de votre AMI afin que le fichier possède l'adresse du serveur de noms DNS IPv6 immédiatement au démarrage.

Lorsque vous lancez votre instance, vous pouvez le faire dans un sous-réseau associé à l'une des ressources suivantes :

- Une zone de disponibilité - Il s'agit de l'option par défaut.
- Une zone locale - Pour lancer une instance dans une zone locale, vous devez vous inscrire à la zone locale, puis créer un sous-réseau dans la zone. Pour plus d'informations, voir [Commencer avec les zones locales](#)
- Une zone Wavelength - Pour lancer une instance dans une zone Wavelength, vous devez choisir la zone Wavelength, puis créer un sous-réseau dans la zone. Pour plus d'informations sur le lancement d'une instance dans une zone Wavelength, consultez [Get started with AWS Wavelength](#).
- Un Outpost - Pour lancer une instance dans un Outpost, vous devez créer un Outpost. Pour plus d'informations sur la création d'un avant-poste, voir [Commencer avec AWS Outposts](#).

Une fois que vous avez lancé votre instance, vous pouvez la connecter et l'utiliser. Au début, l'état de l'instance est `pending`. Lorsque l'état de l'instance indique `running`, cela signifie que le démarrage de l'instance a commencé. Il peut y avoir un bref délai avant que vous puissiez vous connecter à l'instance. Notez que le lancement de types d'instances de matériel nu peut prendre plus de temps.

L'instance reçoit un nom DNS public que vous pouvez utiliser pour la contacter depuis Internet. L'instance reçoit également un nom DNS privé que d'autres instances au sein du même VPC peuvent utiliser pour la contacter.

Lorsque vous n'avez plus besoin d'utiliser une instance, veillez à la mettre hors service. Pour plus d'informations, consultez [Mettre fin aux instances Amazon EC2](#).

Lancer une instance à l'aide du nouvel assistant de lancement d'instance

Vous pouvez lancer une instance à l'aide du nouvel assistant de lancement d'instance. L'assistant de lancement d'instance spécifie les paramètres de lancement qui sont requis pour lancer une instance.

Lorsque l'assistant de lancement d'instance fournit une valeur par défaut, vous pouvez accepter la valeur par défaut ou spécifier votre propre valeur. Si vous acceptez les valeurs par défaut, il est possible de lancer une instance en sélectionnant uniquement une paire de clés.

Important

Lorsque vous lancez une instance qui ne fait pas partie de l'[offre gratuite AWS](#), la durée d'exécution de l'instance vous est facturée, même si celle-ci reste inactive.

Rubriques

- [Lancer rapidement une instance](#)
- [Lancer une instance à l'aide de paramètres définis](#)
- [Lancer une instance à l'aide de l'ancien assistant de lancement d'instance](#)

Lancer rapidement une instance

Pour configurer une instance rapidement à des fins de test, procédez comme suit. Vous allez sélectionner le système d'exploitation et votre paire de clés et accepter les valeurs par défaut. Pour obtenir des informations sur tous les paramètres de l'assistant de lancement d'instance, consultez [Lancer une instance à l'aide de paramètres définis](#).

Pour lancer rapidement une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation en haut de l'écran, la AWS région actuelle est affichée (par exemple, USA East (Ohio)). Sélectionnez une région dans laquelle lancer l'instance. Ce choix est important car certaines ressources Amazon EC2 peuvent être partagées entre des régions, contrairement à d'autres ressources. Pour plus d'informations, consultez [Emplacements des ressources](#).
3. Sur le tableau de bord de la console Amazon EC2, sélectionnez Launch instance (Lancer une instance).
4. (Facultatif) Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom descriptif pour votre instance.

5. Sous Application and OS Images (Amazon machine Image) (Images d'applications et de systèmes d'exploitation (Amazon machine Image)), choisissez Quick Start (Démarrage rapide), puis choisissez le système d'exploitation de votre instance.
6. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou créez-en une.
7. Dans le panneau Summary (Récapitulatif), sélectionnez Launch instance (Lancer l'instance).

Lancer une instance à l'aide de paramètres définis

À l'exception de la paire de clés, l'assistant de lancement d'instance fournit des valeurs par défaut pour tous les paramètres. Vous pouvez accepter la totalité ou une partie des valeurs par défaut, ou configurer une instance en spécifiant vos propres valeurs pour chaque paramètre. Les paramètres sont regroupés dans l'assistant de lancement d'instance. Les instructions suivantes vous guident dans chaque groupe de paramètres.

Paramètres pour la configuration d'instance

- [Commencer le lancement de l'instance](#)
- [Noms et identifications](#)
- [Images d'applications et de systèmes d'exploitation \(Amazon Machine Image\)](#)
- [Type d'instance](#)
- [Paire de clés \(connexion\)](#)
- [Paramètres réseau](#)
- [Configurer le stockage](#)
- [Détails avancés](#)
- [Récapitulatif](#)

Commencer le lancement de l'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation en haut de l'écran, la AWS région actuelle est affichée (par exemple, USA East (Ohio)). Sélectionnez une région dans laquelle lancer l'instance. Ce choix est important car certaines ressources Amazon EC2 peuvent être partagées entre des régions, contrairement à d'autres ressources. Pour plus d'informations, consultez [Emplacements des ressources](#).

3. Sur le tableau de bord de la console Amazon EC2, sélectionnez Launch instance (Lancer une instance).

Noms et identifications

Le nom de l'instance est une identification, où la clé est Name (Nom), et la valeur est le nom que vous spécifiez. Vous pouvez étiqueter l'instance, les volumes et les interfaces réseau. Pour les instances Spot, vous pouvez baliser uniquement la demande d'instance Spot. Pour plus d'informations sur les balises, consultez [Baliser vos ressources Amazon EC2](#).

La spécification d'un nom d'instance et d'identifications supplémentaires est facultative.

- Pour Name (Nom), saisissez un nom descriptif pour l'instance. Si vous ne spécifiez pas de nom, l'instance peut être identifiée par son ID, qui est automatiquement généré lorsque vous lancez l'instance.
- Pour ajouter des identifications supplémentaires, sélectionnez Add additional tags (Ajouter des identifications supplémentaires). Choisissez Add tag (Ajouter une identification), saisissez une clé et une valeur, puis sélectionnez le type de ressource à étiqueter. Choisissez Add tag (Ajouter une identification) pour chaque étiquette supplémentaire.

Images d'applications et de systèmes d'exploitation (Amazon Machine Image)

Une Amazon Machine Image (AMI) contient les informations requises pour créer une instance. Par exemple, une AMI peut contenir le logiciel requis pour agir en tant que serveur Web, tel que Linux, Apache et votre site Web.

Vous pouvez trouver une AMI appropriée en procédant comme suit. Avec chaque option de recherche d'AMI, choisissez Cancel (Annuler) (en haut à droite) pour revenir à l'assistant de lancement d'instance sans choisir une AMI.

Barre de recherche

Pour effectuer une recherche parmi toutes les AMI disponibles, saisissez un mot-clé dans la barre de recherche d'AMI, puis appuyez sur Entrée. Pour sélectionner une AMI, choisissez Select (Sélectionner).

Recents (Récentes)

Les AMI que vous avez récemment utilisées.

Choisissez **Recently launched** (Lancées récemment) ou **Currently in use** (Actuellement en cours d'utilisation), puis, à partir de **Amazon Machine Image (AMI)**, sélectionnez une AMI.

Mes AMI

Les AMI privées que vous possédez ou qui ont été partagées avec vous.

Choisissez **Owned by me** (M'appartenant) ou **Shared with me** (Partagées avec moi), puis, à partir de **Amazon Machine Image (AMI)**, sélectionnez une AMI.

Quick Start

Les AMI sont regroupées par système d'exploitation afin de vous aider à démarrer rapidement.

Sélectionnez d'abord le système d'exploitation dont vous avez besoin, puis dans **Amazon Machine Image (AMI)**, sélectionnez une AMI. Pour sélectionner une AMI éligible pour l'offre gratuite, assurez-vous que l'AMI indique **Free tier eligible** (Éligible à l'offre gratuite).

Browse more AMIs (Parcourir plus d'AMI)

Choisissez **Browse more AMIs (Parcourir plus d'AMI)** pour parcourir le catalogue complet des AMI.

- Pour effectuer une recherche parmi toutes les AMI disponibles, saisissez un mot-clé dans la barre de recherche, puis appuyez sur **Entrée**.
- Pour rechercher une AMI à l'aide d'un paramètre **Systems Manager**, sélectionnez le bouton fléché à droite de la barre de recherche, puis choisissez **Search by Systems Manager parameter** (Rechercher par paramètre **Systems Manager**). Pour plus d'informations, consultez [Rechercher une AMI à l'aide d'un paramètre de Systems Manager](#).
- Pour effectuer une recherche par catégorie, choisissez **Quickstart AMIs** (AMI de démarrage rapide), **My AMIs** (Mes AMI), **AMIs (AMI)**, **AWS Marketplace** ou **Community AMIs** (AMI de la communauté).

AWS Marketplace Il s'agit d'une boutique en ligne où vous pouvez acheter des logiciels qui fonctionnent sur **AWS**, y compris des AMI. Pour plus d'informations sur le lancement d'une instance depuis le **AWS Marketplace**, consultez [Lancer une AWS Marketplace instance](#). Dans **Community AMIs** (AMI de la communauté), vous pouvez trouver des AMI mises à la disposition de la communauté **AWS** par d'autres membres. Les AMI détenues par Amazon ou par un partenaire Amazon vérifié sont certifiées **Fournisseur vérifié**.

- Pour filtrer la liste des AMI, cochez une ou plusieurs cases sous **Refine results** (Affiner les résultats) sur la gauche de l'écran. Les options de filtre sont différentes selon la catégorie de recherche sélectionnée.

- Vérifiez le Type de périphérique racine spécifié pour chaque AMI. Déterminez les types d'AMI dont vous avez besoin, ebs (basées sur Amazon EBS) ou instance-store (basées sur le stockage d'instances). Pour plus d'informations, consultez [Stockage pour le périphérique racine](#).
- Vérifiez le Type de virtualisation spécifié pour chaque AMI. Déterminez le type d'AMI dont vous avez besoin, hvm ou paravirtual. Par exemple, certains types d'instance requièrent HVM. Pour plus d'informations sur les types de virtualisation Linux, consultez [Types de virtualisation AMI](#).
- Vérifiez le mode de démarrage répertorié pour chaque AMI. Notez quelles AMI utilisent le mode de démarrage dont vous avez besoin : legacy-bios, uefi ou uefi-preferred. Pour plus d'informations, consultez [Modes de démarrage Amazon EC2](#).
- Choisissez une AMI correspondant à vos besoins, puis choisissez Sélectionner.

Avertissement lors de la modification de l'AMI

Si vous modifiez la configuration de volumes ou groupes de sécurité associés à l'AMI sélectionnée, puis que vous choisissez une autre AMI, une fenêtre s'ouvre pour vous avertir que certains de vos paramètres actuels seront modifiés ou supprimés. Vous pouvez consulter les modifications apportées aux groupes de sécurité et aux volumes. En outre, vous pouvez soit afficher quels volumes seront ajoutés et supprimés, soit afficher uniquement les volumes qui seront ajoutés.

Type d'instance

Le type d'instance définit la configuration matérielle et la taille de l'instance. Les types d'instance plus importants disposent de plus d'UC et de mémoire. Pour plus d'informations, consultez la section Types d'[instances Amazon EC2](#).

- Pour Instance type (Type d'instance), sélectionnez le type de l'instance.

Niveau gratuit : si votre AWS compte date de moins de 12 mois, vous pouvez utiliser Amazon EC2 dans le cadre du niveau gratuit en sélectionnant le type d'instance t2.micro (ou le type d'instance t3.micro dans les régions où t2.micro n'est pas disponible). Si un type d'instance est éligible dans le cadre du niveau gratuit, il est étiqueté Free tier éligible (Éligible à l'offre gratuite). Pour plus d'informations sur t2.micro et t3.micro, consultez [Instance de performance à capacité extensible](#).

- Comparaison des types d'instances : vous pouvez comparer différents types d'instances en fonction des attributs suivants : nombre de vCPU, architecture, quantité de mémoire (Go), quantité de stockage (Go), type de stockage et performance réseau.

- Obtenir des conseils : vous pouvez obtenir des conseils et des suggestions concernant les types d'instances depuis le sélecteur de type d'instance Amazon Q EC2. Pour plus d'informations, consultez [Obtention de recommandations sur le type d'instance pour une nouvelle charge de travail](#).

Paire de clés (connexion)

Pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou choisissez Create new key pair (Créer une nouvelle paire de clés) pour en créer une nouvelle. Pour plus d'informations, consultez [Paires de clés Amazon EC2 et instances Amazon EC2](#).

Important

Si vous sélectionnez l'option Proceed without key pair (Not recommended) ((Continuer sans paire de clé) (Non recommandé)), vous ne pourrez pas vous connecter à l'instance à moins de choisir une AMI configurée de façon à autoriser les utilisateurs à se connecter d'une autre façon.

Paramètres réseau

Configurez les paramètres réseau, le cas échéant.

- VPC : choisissez un VPC existant pour votre instance. Vous pouvez choisir le VPC par défaut ou un VPC que vous avez créé. Pour plus d'informations, consultez [the section called "Clouds privés virtuels"](#).
- Sous-réseau : vous pouvez lancer une instance dans un sous-réseau associé à une zone de disponibilité, une zone locale, une zone Wavelength ou un Outpost.

Pour lancer l'instance dans une zone de disponibilité, sélectionnez le sous-réseau dans lequel lancer votre instance. Pour créer un sous-réseau, choisissez Créer un nouveau sous-réseau afin d'accéder à la console Amazon VPC. Une fois que vous avez terminé, revenez dans l'assistant de lancement d'instance et choisissez l'icône Refresh (Actualiser) afin de charger votre sous-réseau dans la liste.

Pour lancer l'instance dans un sous-réseau IPv6 uniquement, l'instance doit être [créée sur le système Nitro](#).

Pour lancer l'instance dans une zone locale, sélectionnez un sous-réseau que vous avez créé dans la zone locale.

Pour lancer une instance dans un Outpost, sélectionnez un sous-réseau dans un VPC que vous avez associé à l'Outpost.

- Attribuer automatiquement l'adresse IP publique : indiquez si l'instance est associée à une adresse IPv4 publique. Par défaut, les instances d'un sous-réseau par défaut se voient attribuer une adresse IPv4 publique, contrairement aux instances d'un sous-réseau personnalisé. Vous pouvez sélectionner Activer ou Désactiver pour remplacer la configuration par défaut du sous-réseau. Pour plus d'informations, consultez [Adresses IPv4 publiques](#).
- Firewall (security groups) (Pare-feu (groupes de sécurité)) : utilisez un groupe de sécurité afin de définir les règles de pare-feu de votre instance. Ces règles déterminent le trafic réseau entrant acheminé vers votre instance. Le reste du trafic est ignoré. Pour plus d'informations sur les groupes de sécurité, consultez [Groupes de sécurité Amazon EC2 pour vos instances EC2](#).

Si vous ajoutez une interface réseau, vous devez indiquer le même groupe de sécurité dans l'interface réseau.

Sélectionnez ou créez un groupe de sécurité de la façon suivante :

- Pour sélectionner un groupe de sécurité existant pour votre VPC, choisissez Select existing security group (Sélectionner un groupe de sécurité existant), puis sélectionnez votre groupe de sécurité dans Common security groups (Groupes de sécurité courants).
- Pour créer un nouveau groupe de sécurité pour votre VPC, sélectionnez Create security group (Créer un groupe de sécurité). L'assistant de lancement d'instance définit automatiquement le groupe de sécurité launch-wizard-x et fournit les cases à cocher suivantes pour ajouter rapidement des règles de groupe de sécurité :

(Linux) Autoriser le trafic SSH en provenance de — Crée une règle entrante pour vous permettre de vous connecter à votre instance via SSH (port 22).

(Windows) Autoriser le trafic RDP en provenance de : crée une règle entrante pour vous permettre de vous connecter à votre instance via RDP (port 3389).

Spécifiez si le trafic provient de Anywhere (N'importe où), Custom (Personnalisée), ou My IP (Mon IP).

Autorise le trafic HTTPS à partir d'Internet : crée une règle entrante qui ouvre le port 443 (HTTPS) pour autoriser le trafic Internet depuis n'importe où. Si votre instance est un serveur web, vous aurez besoin de cette règle.

Autorise le trafic HTTP à partir d'Internet : crée une règle entrante qui ouvre le port 80 (HTTP) pour autoriser le trafic Internet depuis n'importe où. Si votre instance est un serveur web, vous aurez besoin de cette règle.

Vous pouvez modifier ces règles et ajouter des règles en fonction de vos besoins.

Pour modifier ou ajouter une règle, choisissez Edit (Modifier) (en haut à droite). Pour ajouter une règle, choisissez Add security group rule (Ajouter une règle de groupe de sécurité). Pour Type, sélectionnez le type de trafic réseau. Le champ Protocol (Protocole) est automatiquement rempli avec le protocole pour s'ouvrir au trafic réseau. Pour Source type (Type de source), sélectionnez le type de source. Sélectionnez My IP (Mon adresse IP) afin de permettre à l'assistant de lancement d'instance d'ajouter l'adresse IP publique de votre ordinateur. Toutefois, si votre connexion s'effectue via un ISP ou derrière un pare-feu sans adresse IP statique, vous devez déterminer la plage d'adresses IP utilisée par les ordinateurs clients.

Warning

Les règles qui activent toutes les adresses IP (0.0.0.0/0) pour accéder à votre instance via SSH ou RDP sont acceptables si vous lancez brièvement une instance de test et que vous l'arrêtez ou la résiliez bientôt, mais ne sont pas acceptables pour un environnement de production. Veillez à autoriser une seule adresse IP ou plage d'adresses à accéder à votre instance.

- Advanced network configuration (Configuration réseau avancée) : disponible uniquement si vous choisissez un sous-réseau.

Interface réseau

- Device index (Index de périphérique) : l'index de la carte réseau. L'interface réseau principale doit être affectée à l'index de carte réseau 0. Certains types d'instance prennent en charge plusieurs cartes réseau.
- Network interface (Interface réseau) : sélectionnez New interface (Nouvelle interface) pour permettre à Amazon EC2 de créer une nouvelle interface, ou sélectionnez une interface réseau disponible et existante.

- Description : (facultatif) description de la nouvelle interface réseau.
- Subnet (Sous-réseau) : sous-réseau dans lequel créer une nouvelle interface réseau. Pour l'interface réseau principale (eth0), il s'agit du sous-réseau dans lequel l'instance est lancée. Si vous avez indiqué une interface réseau existante pour eth0, l'instance est lancée dans le sous-réseau dans lequel l'interface réseau est située.
- Groupes de sécurité : un ou plusieurs groupes de sécurité de votre VPC auxquels associer l'interface réseau.
- IP principale : une adresse IPv4 privée de la plage d'adresses de votre sous-réseau. Laissez ce champ vide pour qu'Amazon EC2 choisisse une adresse IPv4 privée à votre place.
- Secondary IP (Adresse IP secondaire) : une ou plusieurs adresses IPv4 privées supplémentaires de la plage d'adresses de votre sous-réseau. Choisissez Manually assign (Attribuer manuellement) et saisissez une adresse IP. Choisissez Add IP (Ajouter une adresse IP) pour ajouter une autre adresse IP. Sinon, choisissez Automatically assign (Attribuer automatiquement) pour laisser Amazon EC2 en choisir une pour vous et saisissez une valeur indiquant le nombre d'adresses IP à ajouter.
- (IPv6 uniquement) Adresses IP IPv6 : adresse IPv6 comprise dans la plage du sous-réseau. Choisissez Manually assign (Attribuer manuellement) et saisissez une adresse IP. Choisissez Add IP (Ajouter une adresse IP) pour ajouter une autre adresse IP. Sinon, choisissez Automatically assign (Attribuer automatiquement) pour laisser Amazon EC2 en choisir une pour vous et saisissez une valeur indiquant le nombre d'adresses IP à ajouter.
- Préfixes IPv4 : les préfixes IPv4 pour l'interface réseau.
- Préfixes IPv6 : les préfixes IPv6 pour l'interface réseau.
- (Double pile et IPv6 uniquement) Attribuer une adresse IP IPv6 principale : (facultatif) si vous lancez une instance sur un sous-réseau à double pile ou uniquement IPv6, vous avez la possibilité d'Attribuer une adresse IP IPv6 principale. L'attribution d'une adresse IPv6 principale vous permet d'éviter de perturber le trafic vers les instances ou les ENI. Choisissez Activer si cette instance dépend du fait que son adresse IPv6 ne change pas. Lorsque vous lancez l'instance, une adresse IPv6 associée à l'ENI attachée à votre instance AWS sera automatiquement attribuée comme adresse IPv6 principale. Une fois que vous avez activé une adresse GUA IPv6 comme adresse IPv6 principale, vous ne pouvez pas la désactiver. Lorsque vous activez une adresse GUA IPv6 comme adresse IPv6 principale, la première GUA IPv6 devient l'adresse IPv6 principale jusqu'à ce que l'instance soit résiliée ou que l'interface réseau soit détachée. Si plusieurs adresses IPv6 sont associées à une ENI attachée à votre instance et que vous activez une adresse IPv6 principale, la première adresse GUA IPv6 associée à l'ENI devient l'adresse IPv6 principale.

- Supprimer à la résiliation : indiquez s'il convient de supprimer l'interface réseau à la suppression de l'instance.
- Elastic Fabric Adapter (EFA) : Indique si l'interface réseau est une Elastic Fabric Adapter (EFA). Pour plus d'informations, consultez [Elastic Fabric Adapter](#).
- ENA Express : ENA Express est alimenté par la technologie AWS Scalable Reliable Datagram (SRD). La technologie SRD utilise un mécanisme de pulvérisation de paquets pour répartir la charge et éviter la congestion du réseau. L'activation d'ENA Express permet aux instances prises en charge de communiquer en utilisant le SRD en plus du trafic TCP normal lorsque cela est possible. L'assistant de lancement d'instance n'inclut pas la configuration ENA Express pour l'instance, sauf si vous sélectionnez Activer ou Désactiver dans la liste.
- ENA Express UDP : si vous avez activé ENA Express, vous pouvez éventuellement l'utiliser pour le trafic UDP. L'assistant de lancement d'instance n'inclut pas la configuration ENA Express pour l'instance, sauf si vous sélectionnez Activer ou Désactiver.

Choisissez Ajouter une interface réseau pour ajouter des interfaces réseau supplémentaires. Des interfaces réseau supplémentaires peuvent résider dans un sous-réseau différent du même VPC ou dans un sous-réseau d'un autre VPC que vous possédez (à condition que le sous-réseau se trouve dans la même zone de disponibilité que votre instance). Si vous choisissez d'ajouter une interface réseau supplémentaire résidant dans un autre sous-réseau VPC, l'option Sous-réseaux multi-VPC s'affiche lorsque vous sélectionnez un sous-réseau. Si vous sélectionnez un sous-réseau dans un autre VPC, l'étiquette Multi-VPC apparaît à côté de l'interface réseau que vous avez ajoutée. Cela vous permet de créer des instances multi-résidents entre des VPC dotés de différentes configurations réseau et de sécurité. Notez que si vous attachez une ENI supplémentaire depuis un autre VPC, vous devez choisir un groupe de sécurité pour l'ENI à partir de ce VPC.

Pour plus d'informations, consultez [Interfaces réseau Elastic](#). Si vous spécifiez plusieurs interfaces réseau, votre instance ne peut recevoir aucune adresse IPv4 publique. En outre, si vous spécifiez une interface réseau existante pour eth0, vous ne pouvez pas remplacer le paramètre d'adresse IPv4 publique du sous-réseau à l'aide de Attribuer automatiquement l'adresse IP publique. Pour plus d'informations, consultez [Attribuer une adresse IPv4 publique lors du lancement d'une instance](#).

Configurer le stockage

L'AMI sélectionnée inclut un ou plusieurs volumes de stockage, notamment le volume racine. Vous pouvez spécifier d'autres volumes à attacher à l'instance.

Vous pouvez utiliser la vue Simple ou Advanced (Avancée). Avec la vue Simple, vous spécifiez la taille et le type du volume. Pour spécifier tous les paramètres de volume, choisissez la vue Advanced (Avancée) (en haut à droite de la carte).

En utilisant la vue Advanced (Avancée), vous pouvez configurer chaque volume comme suit :

- **Storage type (Type de stockage)** : sélectionnez les volumes de stockage d'instances ou Amazon EBS à associer à votre instance. Les types de volumes disponibles dans la liste dépendent du type d'instance que vous avez sélectionné. Pour plus d'informations, consultez [Stockage d'instances Amazon EC2](#) et [volumes Amazon EBS](#).
- **Device name (Nom du dispositif)** : sélectionnez le périphérique dans la liste des noms de périphériques disponibles pour le volume.
- **Snapshot (Instantané)** : saisissez l'instantané à partir duquel vous souhaitez restaurer le volume. Vous pouvez rechercher les instantanés partagés et publics disponibles en saisissant un texte dans le champ Snapshot (Instantané).
- **Size (GiB) (Taille (Gio))** : pour les volumes EBS, vous pouvez spécifier une taille de stockage. Si vous avez sélectionné une AMI et une instance éligibles pour l'offre gratuite, n'oubliez pas que pour ne pas dépasser les limites de celle-ci, vous devez veiller à ne pas dépasser 30 GiO de stockage au total.
- **Volume type (Type de volume)** : pour les volumes EBS, sélectionnez un type de volume. Pour plus d'informations, consultez les [types de volumes Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.
- **IOPS** : si vous avez sélectionné le type de volume Provisioned IOPS SSD, vous pouvez saisir le nombre d'opérations d'I/O par seconde (IOPS) que le volume peut prendre en charge.
- **Delete on termination (Supprimer à la résiliation)** : pour les volumes Amazon EBS, choisissez Yes (Oui) afin de supprimer le volume lors de la résiliation de l'instance ou No (Non) afin de conserver le volume. Pour plus d'informations, consultez [Conservation des données lors de la résiliation d'une instance](#).
- **Encrypted (Chiffré)** : si le type d'instance prend en charge le chiffrement EBS, vous pouvez sélectionner Yes (Oui) pour activer le chiffrement du volume. Si vous avez activé le chiffrement par défaut dans cette région, le chiffrement est activé automatiquement. Pour plus d'informations,

consultez la section relative au [chiffrement Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

- **KMS Key (Clé KMS)** : si vous avez sélectionné Yes (Oui) pour Encrypted (Chiffré), vous devez ensuite sélectionner une clé gérée par le client à utiliser pour chiffrer le volume. Si vous avez activé le chiffrement par défaut dans cette région, la clé gérée par le client par défaut est sélectionnée pour vous. Vous pouvez sélectionner une clé différente ou spécifier l'ARN de n'importe quelle clé gérée par le client que vous avez créée.
- **Systèmes de fichiers** : montez un système de fichiers Amazon EFS ou Amazon FSx sur l'instance. Pour plus d'informations sur le montage d'un système de fichiers Amazon EFS, consultez [Utiliser Amazon EFS avec des instances Linux](#). Pour plus d'informations sur le montage d'un système de fichiers Amazon FSx, consultez [Utiliser Amazon FSx avec Amazon EC2](#).

Détails avancés

Développez la section Détails avancés pour afficher les champs et spécifier des paramètres supplémentaires pour l'instance.

- **Purchasing option (Option d'achat)** : choisissez Request Spot Instances (Demander des instances Spot) pour demander des instances Spot au prix Spot, plafonné au prix à la demande, et choisissez Customize (Personnaliser) pour modifier les paramètres par défaut de l'instance Spot. Vous pouvez définir votre prix maximum (non recommandé) et modifier le type de demande, la durée de la demande et le comportement d'interruption. Si vous ne demandez pas une instance Spot, Amazon EC2 lance une instance à la demande par défaut. Pour plus d'informations, consultez [Créer une demande d'instance Spot](#).
- **Répertoire de jointure de domaines** : sélectionnez le AWS Directory Service répertoire (domaine) auquel votre instance est jointe après le lancement. Si vous sélectionnez un domaine, vous devez sélectionner un rôle IAM avec les autorisations requises. Pour plus d'informations sur la jonction d'instances Linux à un domaine, voir [Joindre facilement une instance Linux EC2 à votre répertoire Microsoft AD AWS géré](#). Pour plus d'informations sur la jonction d'instances Windows à un domaine, voir [Joindre facilement une instance Windows EC2 à votre répertoire Microsoft AD AWS géré](#).
- **Profil d'instance IAM** : sélectionnez un profil d'instance AWS Identity and Access Management (IAM) à associer à l'instance. Pour plus d'informations, consultez [Rôles IAM pour Amazon EC2](#).
- **Hostname type (Type de nom d'hôte)** : sélectionnez si le nom d'hôte du système d'exploitation hôte de l'instance inclura le nom de la ressource ou le nom de l'adresse IP. Pour plus d'informations, consultez [Types de noms d'hôtes des instances Amazon EC2](#).

- DNS Hostname(Nom d'hôte DNS) : détermine si les requêtes DNS relatives au nom de la ressource ou au nom de l'adresse IP (selon votre choix pour Hostname type [Type de nom d'hôte]) répondront à l'aide de l'adresse IPv4 (registre A), de l'adresse IPv6 (registre AAAA), ou des deux. Pour plus d'informations, consultez [Types de noms d'hôtes des instances Amazon EC2](#).
- Comportement d'arrêt : indiquez si l'instance doit s'arrêter ou être résiliée lorsque vous arrêtez l'ordinateur. Pour plus d'informations, consultez [Modifier le comportement d'arrêt lancé de l'instance](#).
- Stop - Hibernate behavior (Comportement d'arrêt - mise en veille prolongée) : pour activer la mise en veille prolongée, sélectionnez Enable (Activer). Ce champ est uniquement disponible si votre instance satisfait les conditions préalables à la mise en veille prolongée. Pour plus d'informations, consultez [Hibernez votre instance Amazon EC2](#).
- Termination protection (Protection de la résiliation) : pour éviter toute mise hors service accidentelle, sélectionnez Enable (Activer). Pour plus d'informations, consultez [Activer la protection de la résiliation](#).
- Stop protection (Protection contre l'arrêt) : pour éviter tout arrêt accidentel, choisissez Enable (Activer). Pour plus d'informations, consultez [Activer la protection contre l'arrêt](#).
- CloudWatch Surveillance détaillée : choisissez Activer pour activer la surveillance détaillée de votre instance à l'aide d'Amazon CloudWatch. Des frais supplémentaires seront facturés. Pour plus d'informations, consultez [Surveillez vos instances à l'aide de CloudWatch](#).
- GPU élastique : Amazon Elastic Graphics a atteint la fin de son cycle de vie le 8 janvier 2024. Pour les charges de travail nécessitant une accélération graphique, nous vous recommandons d'utiliser des instances Amazon EC2 G4ad, G4dn ou G5.
- Elastic inference (Inférence Elastic) : accélérateur d'inférence Elastic à attacher à votre instance de CPU EC2. Pour plus d'informations, consultez [Utilisation d'Amazon Elastic Inference](#) dans le Guide du développeur Amazon Elastic Inference.

Note

À compter du 15 avril 2023, AWS nous n'intégrerons pas de nouveaux clients à Amazon Elastic Inference (EI) et nous aiderons les clients actuels à migrer leurs charges de travail vers des options offrant un meilleur prix et de meilleures performances. Après le 15 avril 2023, les nouveaux clients ne pourront plus lancer d'instances avec les accélérateurs Amazon EI sur Amazon SageMaker, Amazon ECS ou Amazon EC2. Toutefois, les clients qui ont utilisé Amazon EI au moins une fois au cours des 30 derniers jours sont considérés comme des clients actuels et pourront continuer à utiliser le service.

- **Credit specification (Spécification de crédit)** : sélectionnez Unlimited (Non limité) pour permettre aux applications de s'exécuter au-delà du niveau de référence aussi longtemps que nécessaire. Ce champ est valable uniquement pour les instances T. Des frais supplémentaires peuvent être facturés. Pour plus d'informations, consultez [Instance de performance à capacité extensible](#).
- **Nom du groupe de placement** : indiquez un groupe de placement dans lequel lancer l'instance. Vous pouvez sélectionner un groupe de placement existant ou en créer un nouveau. Le lancement dans un groupe de placement n'est pas possible pour tous les types d'instance. Pour plus d'informations, consultez [Groupes de placement](#).
- **EBS-optimized instance (Instance optimisée pour EBS)** : une instance qui est optimisée pour Amazon EBS a recours à une pile de configuration optimisée et fournit une capacité supplémentaire dédiée pour les I/O Amazon EBS. Si le type d'instance prend en charge cette fonction, sélectionnez Enable (Activer) pour l'activer. Des frais supplémentaires seront facturés. Pour plus d'informations, consultez [the section called "Optimisation EBS"](#).
- **Capacity Reservation (Réserve de capacité)** : indiquez s'il convient de lancer l'instance dans une réserve de capacité (Open (Ouvrir)), dans une réserve de capacité spécifique (Target by ID (Cibler par ID)) ou dans un groupe de réserve de capacité (Target by group (Cibler par groupe)). Pour spécifier qu'il ne faut pas utiliser de réserve de capacité, choisissez None (Aucune). Pour plus d'informations, consultez [Lancer des instances dans une Réserve de capacité existante](#).
- **Location** : indiquez s'il convient d'exécuter votre instance sur un matériel partagé (Partagé), isolé, dédié (Dédié) ou sur un Hôte dédié (Hôte dédié). Si vous choisissez de lancer l'instance sur un Hôte dédié, vous pouvez spécifier si l'instance doit être lancée dans un groupe de ressources hôte ou vous pouvez cibler un Hôte dédié spécifique. Des frais supplémentaires peuvent être facturés. Pour plus d'informations, consultez [Dedicated instances](#) et [Hôtes dédiés](#).
- **RAM disk ID (ID de disque RAM)** : (valide uniquement pour les AMI paravirtuelles (PV)) Sélectionnez un disque RAM pour l'instance. Si vous avez sélectionné un noyau, vous devrez peut-être sélectionner un disque RAM spécifique avec les pilotes qui l'accompagnent.
- **Kernel ID (ID du noyau)** : (valide uniquement pour les AMI paravirtuelles (PV)) Sélectionnez un noyau pour l'instance.
- **Nitro Enclave** : permet de créer des environnements d'exécution isolés, appelés enclaves, à partir d'instances Amazon EC2. Sélectionnez Activer pour activer l'instance pour AWS Nitro Enclaves. Pour plus d'informations, consultez [Qu'est-ce que AWS Nitro Enclaves ?](#) dans le guide de l'utilisateur de AWS Nitro Enclaves.
- **Configurations de licence** : vous pouvez lancer des instances sur la configuration de licence spécifiée pour suivre l'utilisation de votre licence. Pour plus d'informations, consultez [Create a](#)

[License Configuration](#) (Création d'une configuration de licence) dans le Guide de l'utilisateur AWS License Manager.

- Metadata accessible (Métadonnées accessibles) : vous pouvez activer ou désactiver l'accès aux métadonnées de l'instance. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les nouvelles instances](#).
- Point de terminaison IPv6 des métadonnées : vous pouvez autoriser l'instance à utiliser l'adresse IPv6 IMDS [fd00:ec2::254] pour récupérer les métadonnées de l'instance. Cette option n'est disponible que si vous lancez [des instances basées sur le système AWS Nitro](#) dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement). Pour plus d'informations sur la récupération des métadonnées d'instance, consultez [Récupérer des métadonnées d'instance](#).
- Metadata version (Version des métadonnées) : si vous activez l'accès aux métadonnées de l'instance, vous pouvez choisir d'exiger l'utilisation de Service des métadonnées d'instance Version 2 lors de la demande de métadonnées d'instance. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les nouvelles instances](#).
- Limite de sauts de réponse de jeton de métadonnées : si vous activez les métadonnées d'instance, vous pouvez définir le nombre autorisé de sauts réseau pour le jeton de métadonnées. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les nouvelles instances](#).
- Allow tags in metadata (Autoriser les balises dans les métadonnées) : si vous sélectionnez Enable (Activer), l'instance autorise l'accès à toutes ses balises à partir de ses métadonnées. Si aucune valeur n'est spécifiée, l'accès aux identifications dans les métadonnées de l'instance est désactivé par défaut. Pour plus d'informations, consultez [Autoriser l'accès aux identifications dans les métadonnées d'instance](#).
- Données utilisateur : vous pouvez spécifier les données utilisateur pour configurer une instance lors du lancement ou pour exécuter un script de configuration. Pour plus d'informations sur les données utilisateur pour les instances Linux, consultez [Exécutez des commandes sur votre instance Amazon EC2 au lancement](#). Pour plus d'informations sur les données utilisateur pour les instances Windows, consultez [Comment Amazon EC2 gère les données utilisateur pour les instances Windows](#).

Récapitulatif

Utilisez le panneau Summary (Récapitulatif) pour spécifier le nombre d'instances à lancer, vérifier la configuration de votre instance et lancer vos instances.

- Nombre d'instances : entrez le nombre d'instances à lancer. Toutes les instances seront lancées avec la même configuration.

 Tip

Pour accélérer les lancements d'instances, divisez les demandes volumineuses en lots plus petits. Par exemple, créez cinq demandes de lancement distinctes pour 100 instances au lieu d'un lancement pour 500 instances.

- (Facultatif) Si vous spécifiez plus d'une instance, afin d'avoir un nombre suffisant d'instances pour gérer la demande sur votre application, vous pouvez choisir Consider EC2 Auto Scaling (Envisager la scalabilité automatique EC2) pour créer un modèle de lancement et un groupe Auto Scaling. La fonctionnalité Auto Scaling fait évoluer le nombre d'instances du groupe en fonction de vos spécifications. Pour plus d'informations, consultez le [Guide de l'utilisateur Amazon EC2 Auto Scaling](#).

 Note

Si Amazon EC2 Auto Scaling marque une instance qui se trouve dans un groupe Auto Scaling comme non saine, elle est automatiquement planifiée pour le remplacement lorsqu'elle est terminée et qu'une autre est lancée, et vous perdez vos données sur l'instance d'origine. Une instance est marquée comme non saine si vous arrêtez ou redémarrez l'instance, ou si un autre événement marque l'instance comme non saine. Pour plus d'informations, consultez [la section Contrôles de santé des instances d'un groupe Auto Scaling](#) dans le manuel Amazon EC2 Auto Scaling User Guide.

- Vérifiez les détails de votre instance et effectuez les modifications nécessaires. Vous pouvez accéder directement à une section en sélectionnant son lien dans le panneau Summary (Récapitulatif).
- Lorsque vous êtes prêt à lancer votre instance, choisissez Launch instance (Lancer l'instance).

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez [Résoudre les problèmes de lancement d'instance](#).

(Facultatif) Vous pouvez créer une alerte de facturation pour l'instance. Sur l'écran de confirmation, sous Next Steps (Étapes suivantes), choisissez Create billing alerts (Créer des alarmes de contrôle de facturation) et suivez les instructions. Des alertes de facturation peuvent également être créées après le lancement de l'instance. Pour plus d'informations, consultez la section [Création](#)

[d'une alarme de facturation pour surveiller vos AWS frais estimés](#) dans le guide de CloudWatch l'utilisateur Amazon.

Lancer une instance à l'aide de l'ancien assistant de lancement d'instance

Vous pouvez lancer une instance en utilisant l'ancien assistant de lancement d'instance uniquement si votre région prend en charge l'ancienne expérience de lancement. L'assistant de lancement d'instance spécifie tous les paramètres de lancement requis pour lancer une instance. Lorsque l'assistant de lancement d'instance fournit une valeur par défaut, vous pouvez accepter la valeur par défaut ou spécifier votre propre valeur. Vous devez spécifier une AMI et une paire de clés pour lancer une instance.

Pour obtenir les instructions d'utilisation du nouvel assistant de lancement d'instance, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

⚠ Important

Lorsque vous lancez une instance qui ne fait pas partie de l'[offre gratuite AWS](#), la durée d'exécution de l'instance vous est facturée, même si celle-ci reste inactive.

Étapes de lancement d'une instance :

- [Commencer le lancement de l'instance](#)
- [Étape 1 : Sélectionner d'une Amazon Machine Image \(AMI\)](#)
- [Étape 2 : Choisir un type d'instance](#)
- [Étape 3 : Configurer les détails de l'instance](#)
- [Étape 4 : Ajouter du stockage](#)
- [Étape 5 : Ajouter des balises](#)
- [Étape 6 : Configurer un groupe de sécurité](#)
- [Étape 7 : Vérifier le lancement de l'instance et sélectionner une paire de clés](#)

Commencer le lancement de l'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation en haut de l'écran, la région actuelle est affichée (par exemple, US East (Ohio)). Sélectionnez une région pour l'instance répondant à vos besoins. Ce choix

est important car certaines ressources Amazon EC2 peuvent être partagées entre des régions, contrairement à d'autres ressources. Pour plus d'informations, consultez [Emplacements des ressources](#).

3. Sur le tableau de bord de la console Amazon EC2, sélectionnez Launch instance (Lancer une instance).

Étape 1 : Sélectionner d'une Amazon Machine Image (AMI)

Lorsque vous lancez une instance, vous devez sélectionner une configuration connue sous le nom d'Amazon Machine Image (AMI). Une AMI contient les informations nécessaires à la création d'une instance. Par exemple, une AMI peut contenir le logiciel requis pour agir en tant que serveur Web, tel que Linux, Apache et votre site Web.

Lorsque vous lancez une instance, vous pouvez sélectionner une AMI dans la liste ou sélectionner un paramètre Systems Manager pointant vers un ID AMI. Pour plus d'informations, consultez [the section called "Rechercher une AMI à l'aide d'un paramètre de Systems Manager"](#).

Sur la page Choisir une Amazon Machine Image (AMI) utilisez l'une des deux options pour choisir une AMI. [Recherchez la liste des AMI](#), ou [effectuez une recherche par paramètre Systems Manager](#).

En recherchant la liste des AMI

1. Sélectionnez le type d'AMI à utiliser dans le volet gauche :

Quick Start

Quelques AMI couramment utilisées pour vous aider à démarrer rapidement. Pour sélectionner une AMI éligible pour l'offre gratuite, choisissez Offre gratuite uniquement dans le volet gauche. Ces AMI sont indiquées comme Admissible à l'offre gratuite.

Mes AMI

Les AMI privées que vous possédez ou qui ont été partagées avec vous. Pour voir les AMI partagées avec vous, choisissez Shared with me (Partagé avec moi) dans le volet de gauche.

AWS Marketplace

Une boutique en ligne où vous pouvez acheter des logiciels qui s'exécutent sur AWS, y compris des AMI. Pour plus d'informations sur le lancement d'une instance depuis le AWS Marketplace, consultez [Lancer une AWS Marketplace instance](#).

AMI de la communauté

Les AMI que les membres de AWS la communauté ont mises à la disposition des autres utilisateurs. Pour filtrer la liste des AMI par système d'exploitation, activez la case à cocher appropriée sous Système d'exploitation. Vous pouvez également filtrer par architecture et par type d'appareil racine.

2. (Instances Linux) Vérifiez le type de périphérique racine répertorié pour chaque AMI. Déterminez les types d'AMI dont vous avez besoin, soit `ebs` (basé sur Amazon EBS) soit `instance-store` (basé sur le stockage d'instances). Pour plus d'informations, consultez [Stockage pour le périphérique racine](#).
3. Vérifiez le Type de virtualisation spécifié pour chaque AMI. Déterminez le type d'AMI dont vous avez besoin, `hvm` ou `paravirtual`. Par exemple, certains types d'instance requièrent HVM. Pour plus d'informations sur les types de virtualisation Linux, consultez [Types de virtualisation AMI](#).
4. Vérifiez le mode de démarrage répertorié pour chaque AMI. Notez quelles AMI utilisent le mode de démarrage dont vous avez besoin, `legacy-bios` ou `uefi`. Pour plus d'informations, consultez [Modes de démarrage Amazon EC2](#).
5. Choisissez une AMI correspondant à vos besoins, puis choisissez Sélectionner.

Par paramètre Systems Manager

1. Choisissez Rechercher par paramètre Systems Manager (en haut à droite).
2. Pour Paramètre Systems Manager, sélectionnez un paramètre. L'ID AMI correspondant apparaît à côté de Currently resolves to (Se résout en).
3. Choisissez Search (Rechercher). Les AMI correspondant à l'ID AMI apparaissent dans la liste.
4. Sélectionnez l'AMI dans la liste, puis choisissez Select (Sélectionner).

Étape 2 : Choisir un type d'instance

Sur la page Choisir un type d'instance, sélectionnez la configuration matérielle et la taille de l'instance à lancer. Les types d'instance plus importants disposent de plus d'UC et de mémoire. Pour plus d'informations, consultez [Types d'instances Amazon EC2](#).

Pour rester éligible pour l'offre gratuite, choisissez le type d'instance `t2.micro` (ou le type d'instance `t3.micro` dans des régions où `t2.micro` n'est pas disponible). Si un type d'instance est éligible dans

le cadre du niveau gratuit, il est étiqueté Free tier éligible (Éligible à l'offre gratuite). Pour plus d'informations sur t2.micro et t3.micro, consultez [Instance de performance à capacité extensible](#).

Par défaut, l'assistant affiche les types d'instance de la génération actuelle et sélectionne le premier type d'instance disponible en fonction de l'AMI que vous avez sélectionnée. Pour afficher les types d'instances de la génération précédente, choisissez Toutes les générations dans la liste de filtres.

Note

Pour configurer une instance rapidement à des fins de test, choisissez Vérifier et lancer afin d'accepter les paramètres de configuration par défaut, puis lancer votre instance. Sinon, pour configurer votre instance plus en détails, choisissez Suivant : Configurer les détails de l'instance.

Étape 3 : Configurer les détails de l'instance

Sur la page Configurer les détails de l'instance, modifiez les paramètres suivants en fonction de vos besoins (développez Détails avancés pour afficher tous les paramètres), puis choisissez Suivant : Ajouter le stockage :

- Nombre d'instances : entrez le nombre d'instances à lancer.

Tip

Pour accélérer les lancements d'instances, divisez les demandes volumineuses en lots plus petits. Par exemple, créez cinq demandes de lancement distinctes pour 100 instances au lieu d'un lancement pour 500 instances.

- (Facultatif) Afin d'avoir un nombre suffisant d'instances pour gérer la demande sur votre application, vous pouvez choisir Lancer dans un groupe Auto Scaling pour créer une configuration de lancement et un groupe Auto Scaling. La fonctionnalité Auto Scaling fait évoluer le nombre d'instances du groupe en fonction de vos spécifications. Pour plus d'informations, consultez le [Guide de l'utilisateur Amazon EC2 Auto Scaling](#).

Note

Si Amazon EC2 Auto Scaling marque une instance qui se trouve dans un groupe Auto Scaling comme non saine, elle est automatiquement planifiée pour le remplacement

lorsqu'elle est terminée et qu'une autre est lancée, et vous perdez vos données sur l'instance d'origine. Une instance est marquée comme non saine si vous arrêtez ou redémarrez l'instance, ou si un autre événement marque l'instance comme non saine. Pour plus d'informations, consultez [Vérifications de l'état pour les instances Auto Scaling](#) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

- Option d'achat : sélectionnez Demander des instances Spot pour lancer une instance Spot. Cet utilitaire ajoute et supprime des options de cette page. Vous pouvez facultativement définir votre prix maximum (non recommandé), et facultativement changer le type de demande, le comportement d'interruption, et la validité de la demande. Pour plus d'informations, consultez [Créer une demande d'instance Spot](#).
- Réseau : sélectionnez le VPC ou, pour créer un nouveau VPC, choisissez Créer un nouveau VPC afin d'accéder à la console Amazon VPC. Une fois que vous avez terminé, revenez dans l'assistant de lancement d'instance et choisissez Refresh (Actualiser) pour charger votre VPC dans la liste.
- Sous-réseau : vous pouvez lancer une instance dans un sous-réseau associé à une zone de disponibilité, à une zone locale, à une zone Wavelength ou à Outpost.

Pour lancer l'instance dans une zone de disponibilité, sélectionnez le sous-réseau dans lequel lancer votre instance. Vous pouvez sélectionner Aucune préférence pour AWS choisir un sous-réseau par défaut dans n'importe quelle zone de disponibilité. Pour créer un sous-réseau, choisissez Créer un nouveau sous-réseau afin d'accéder à la console Amazon VPC. Une fois que vous avez terminé, revenez dans l'assistant et choisissez Actualiser afin de charger votre sous-réseau dans la liste.

Pour lancer l'instance dans une zone locale, sélectionnez un sous-réseau que vous avez créé dans la zone locale.

Pour lancer une instance dans un Outpost, sélectionnez un sous-réseau dans un VPC que vous avez associé à un Outpost.

- Attribuer automatiquement l'adresse IP publique : indiquez si l'instance est associée à une adresse IPv4 publique. Par défaut, les instances d'un sous-réseau par défaut se voient attribuer une adresse IPv4 publique, contrairement aux instances d'un sous-réseau personnalisé. Vous pouvez sélectionner Activer ou Désactiver pour remplacer la configuration par défaut du sous-réseau. Pour plus d'informations, consultez [Adresses IPv4 publiques](#).
- Attribuer automatiquement l'adresse IP IPv6 : spécifiez si votre instance reçoit une adresse IPv6 de la plage du sous-réseau. Sélectionnez Activer ou Désactiver pour remplacer le paramètre par défaut du sous-réseau. Cette option est uniquement disponible si vous avez associé un bloc

- d'adresses CIDR IPv6 à votre VPC et à votre sous-réseau. Pour plus d'informations, consultez [Ajouter un bloc d'adresse CIDR IPv6 à votre VPC](#) dans le Guide de l'utilisateur Amazon VPC.
- Hostname type (Type de nom d'hôte) : sélectionnez si le nom d'hôte du système d'exploitation hôte de l'instance inclura le nom de la ressource ou le nom de l'adresse IP. Pour plus d'informations, consultez [Types de noms d'hôtes des instances Amazon EC2](#).
 - DNS Hostname(Nom d'hôte DNS) : détermine si les requêtes DNS relatives au nom de la ressource ou au nom de l'adresse IP (selon votre choix pour Hostname type [Type de nom d'hôte]) répondront à l'aide de l'adresse IPv4 (registre A), de l'adresse IPv6 (registre AAAA), ou des deux. Pour plus d'informations, consultez [Types de noms d'hôtes des instances Amazon EC2](#).
 - Répertoire des jointures de domaines : sélectionnez le AWS Directory Service répertoire (domaine) auquel votre instance est jointe après le lancement. Si vous sélectionnez un domaine, vous devez sélectionner un rôle IAM avec les autorisations requises. Pour plus d'informations sur la jonction d'instances Linux à un domaine, voir [Joindre facilement une instance Linux EC2 à votre répertoire Microsoft AD AWS géré](#). Pour plus d'informations sur la jonction de domaines avec des instances Windows, [rejoignez facilement une instance Windows EC2](#).
 - Groupe de placement : un groupe de placement détermine la stratégie de placement de vos instances. Sélectionnez un groupe de placement existant ou créez-en un nouveau. Cette option est disponible uniquement si vous avez sélectionné un type d'instance qui prend en charge les groupes de placement. Pour plus d'informations, consultez [Groupes de placement](#).
 - Réserve de capacité : indiquez s'il convient de lancer l'instance dans la capacité partagée, dans une Réserve de capacité open, une Réserve de capacité spécifique ou un groupe Réserve de capacité. Pour plus d'informations, consultez [Lancer des instances dans une Réserve de capacité existante](#).
 - Rôle IAM : sélectionnez un rôle AWS Identity and Access Management (IAM) à associer à l'instance. Pour plus d'informations, consultez [Rôles IAM pour Amazon EC2](#).
 - CPU options (Options d'UC) : choisissez Specify CPU options (Spécifier les options d'UC) pour spécifier un nombre personnalisé de vCPU lors du lancement. Définissez le nombre de cœurs d'UC et de threads par cœur. Pour plus d'informations, consultez [Optimiser les options d'UC](#).
 - Comportement d'arrêt : indiquez si l'instance doit s'arrêter ou être résiliée lorsque vous arrêtez l'ordinateur. Pour plus d'informations, consultez [Modifier le comportement d'arrêt lancé de l'instance](#).
 - Comportement d'arrêt - mise en veille prolongée : pour activer la mise en veille prolongée, sélectionnez cette case à cocher. Cette option est uniquement disponible si votre instance satisfait les conditions préalables à la mise en veille prolongée. Pour plus d'informations, consultez [Hibernez votre instance Amazon EC2](#).

- Activer la protection de la résiliation : activez cette case à cocher pour éviter toute mise hors service accidentelle. Pour plus d'informations, consultez [Activer la protection de la résiliation](#).
- Enable stop protection (Activer la protection de la résiliation) : pour éviter toute arrêt accidentel, cochez cette case. Pour plus d'informations, consultez [Activer la protection contre l'arrêt](#).
- Surveillance : cochez cette case pour activer la surveillance détaillée de votre instance à l'aide d'Amazon CloudWatch. Des frais supplémentaires seront facturés. Pour plus d'informations, consultez [Surveillez vos instances à l'aide de CloudWatch](#).
- EBS-optimized instance (Instance optimisée pour EBS) : une instance optimisée pour Amazon EBS a recours à une pile de configuration optimisée et fournit une capacité supplémentaire dédiée pour les I/O Amazon EBS. Des frais supplémentaires seront facturés. Pour plus d'informations, consultez [instances optimisées pour Amazon EBS](#).
- Location : si vous lancez votre instance sur un VPC, vous pouvez choisir de l'exécuter sur un matériel isolé dédié (Dédié) ou sur un hôte dédié (Hôte dédié). Des frais supplémentaires peuvent être facturés. Pour plus d'informations, consultez [Dedicated instances](#) et [Hôtes dédiés](#).
- T2/T3 illimité : activez cette case à cocher pour permettre aux applications de s'exécuter au-delà du niveau de référence aussi longtemps que nécessaire. Des frais supplémentaires peuvent être facturés. Pour plus d'informations, consultez [Instance de performance à capacité extensible](#).
- Systèmes de fichiers : pour créer un nouveau système de fichiers à monter sur votre instance, sélectionnez Create new file system (Créer un nouveau système de fichiers), saisissez un nom pour le nouveau système de fichiers, puis cliquez sur Create (Créer). Le système de fichiers est créé à l'aide de la création rapide Amazon EFS, qui applique les paramètres recommandés par le service. Les groupes de sécurité requis pour activer l'accès au système de fichiers sont automatiquement créés et attachés à l'instance et aux cibles de montage du système de fichiers. Vous pouvez également choisir de créer et d'attacher manuellement les groupes de sécurité requis. Pour monter un ou plusieurs systèmes de fichiers Amazon EFS existants sur votre instance, sélectionnez Ajdd file system (Ajouter un système de fichiers), puis choisissez les systèmes de fichiers à monter et les points de montage à utiliser. Pour plus d'informations, consultez [Utiliser Amazon EFS avec des instances Linux](#).
- Interfaces réseau : si vous avez sélectionné un sous-réseau spécifique, vous pouvez spécifier jusqu'à deux interfaces réseau pour votre instance :
 - Pour Interface réseau, sélectionnez Nouvelle interface réseau pour permettre de AWS créer une nouvelle interface, ou sélectionnez une interface réseau existante disponible.
 - Pour l'adresse IP principale, entrez une adresse IPv4 privée dans la plage de votre sous-réseau ou laissez Attribuer automatiquement pour AWS choisir une adresse IPv4 privée pour vous.

- Pour Adresses IP secondaires, choisissez Ajouter l'IP pour affecter plusieurs adresses IPv4 privées à l'interface réseau sélectionnée.
- (IPv6 uniquement) Pour les adresses IP IPv6, choisissez Ajouter une adresse IP et entrez une adresse IPv6 dans la plage du sous-réseau, ou laissez Attribuer automatiquement pour laisser le soin d'en choisir une pour vous AWS .
- Index de carte réseau : l'index de la carte réseau. L'interface réseau principale doit être affectée à l'index de carte réseau 0. Certains types d'instance prennent en charge plusieurs cartes réseau.
- Choisissez Ajouter périphérique pour ajouter une interface réseau secondaire. Une interface réseau secondaire peut résider dans un autre sous-réseau du VPC, à condition que celui-ci figure dans la même zone de disponibilité que votre instance.

Pour plus d'informations, consultez [Interfaces réseau Elastic](#). Si vous spécifiez plusieurs interfaces réseau, votre instance ne peut recevoir aucune adresse IPv4 publique. En outre, si vous spécifiez une interface réseau existante pour eth0, vous ne pouvez pas remplacer le paramètre d'adresse IPv4 publique du sous-réseau à l'aide de Attribuer automatiquement l'adresse IP publique. Pour plus d'informations, consultez [Attribuer une adresse IPv4 publique lors du lancement d'une instance](#).

- ID du noyau : (valide uniquement pour les AMIs paravirtuelles, PV) sélectionnez Utiliser la valeur par défaut sauf si vous souhaitez utiliser un noyau spécifique.
- ID de disque RAM : (valide uniquement pour les AMIs paravirtuelles, PV) sélectionnez Utiliser la valeur par défaut sauf si vous souhaitez utiliser un disque RAM spécifique. Si vous avez sélectionné un noyau, vous devrez peut-être sélectionner un disque RAM spécifique avec les pilotes qui l'accompagnent.
- Enclave : sélectionnez Activer pour activer l'instance pour AWS Nitro Enclaves. Pour plus d'informations, consultez [Qu'est-ce que AWS Nitro Enclaves ?](#) dans le guide de l'utilisateur de AWS Nitro Enclaves.
- Métadonnées accessibles : vous pouvez activer ou désactiver l'accès au service des métadonnées d'instance (IMDS). Pour plus d'informations, consultez [Utiliser IMDSv2](#).
- Point de terminaison IPv6 des métadonnées : vous pouvez autoriser l'instance à utiliser l'adresse IPv6 IMDS [fd00::ec2::254] pour récupérer les métadonnées de l'instance. Cette option n'est disponible que si vous lancez [des instances basées sur le système AWS Nitro](#) dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement). Pour plus d'informations sur la récupération des métadonnées d'instance, consultez [Récupérer des métadonnées d'instance](#).

- **Version des métadonnées** : si vous activez l'accès à l'IMDS, vous pouvez choisir d'exiger l'utilisation du service des métadonnées d'instance Version 2 lors de la demande de métadonnées d'instance. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les nouvelles instances](#).
- **Durée de vie de réponse du jeton de métadonnées** : si vous activez l'IMDS, vous pouvez définir le nombre autorisé de sauts réseau pour le jeton de métadonnées. Pour plus d'informations, consultez [Utiliser IMDSv2](#).
- **Données utilisateur** : vous pouvez spécifier les données utilisateur pour configurer une instance lors du lancement ou pour exécuter un script de configuration. Pour attacher un fichier, sélectionnez l'option Sous forme de fichier et parcourez la liste jusqu'à ce que vous trouviez le fichier à attacher.

Étape 4 : Ajouter du stockage

L'AMI sélectionnée inclut un ou plusieurs volumes de stockage, notamment le volume du périphérique racine. Sur la page Ajouter le stockage, vous pouvez spécifier des volumes supplémentaires à attacher à l'instance en choisissant Ajouter un nouveau volume. Configurez chaque volume comme suit, puis choisissez Suivant : Ajouter des balises.

- **Type** : sélectionnez le stockage d'instances ou les volumes Amazon EBS à associer à votre instance. Les types de volumes disponibles dans la liste dépendent du type d'instance que vous avez sélectionné. Pour plus d'informations, consultez [Stockage d'instances Amazon EC2 et volumes Amazon EBS](#).
- **Dispositif** : sélectionnez l'appareil dans la liste des noms d'appareils disponibles pour le volume.
- **Instantané** : entrez le nom ou l'ID de l'instantané à partir duquel vous souhaitez restaurer un volume. Vous pouvez également rechercher les instantanés partagés et publics disponibles en saisissant un texte dans le champ Instantané. Les descriptions d'instantané sont sensibles à la casse.
- **Taille** : pour les volumes EBS, vous pouvez spécifier une taille de stockage. Même si vous avez sélectionné une AMI et une instance éligibles pour l'offre gratuite, afin de ne pas dépasser les limites de celle-ci, vous devez veiller à ne pas dépasser 30 GiO de stockage au total.
- **Type de volume** : pour les volumes EBS, sélectionnez un type de volume. Pour plus d'informations, consultez les [types de volumes Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.
- **IOPS** : si vous avez sélectionné le type de volume Provisioned IOPS SSD, vous pouvez saisir le nombre d'opérations d'I/O par seconde (IOPS) que le volume peut prendre en charge.

- **Supprimer à la résiliation** : pour les volumes Amazon EBS, activez cette case à cocher afin de supprimer le volume une fois l'instance résiliée. Pour plus d'informations, consultez [Conservation des données lors de la résiliation d'une instance](#).
- **Chiffré** : si le type d'instance prend en charge le chiffrement EBS, vous pouvez spécifier l'état de chiffrement du volume. Si vous avez activé le chiffrement par défaut dans cette région, la clé gérée par le client par défaut est sélectionnée pour vous. Vous pouvez sélectionner une autre clé ou désactiver le chiffrement. Pour plus d'informations, consultez la section relative au [chiffrement Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Étape 5 : Ajouter des balises

Sur la page Ajouter des balises, spécifiez les [balises](#) en fournissant les combinaisons clé et valeur. Vous pouvez attribuer une balise à l'instance, aux volumes ou aux deux. Pour les instances Spot, vous pouvez baliser uniquement la demande d'instance Spot. Choisissez Ajouter une autre balise pour ajouter plusieurs balises à vos ressources. Choisissez Suivant : Configurer le groupe de sécurité une fois que vous avez terminé.

Étape 6 : Configurer un groupe de sécurité

Sur la page Configurer le groupe de sécurité, utilisez un groupe de sécurité afin de définir les règles de pare-feu de votre instance. Ces règles déterminent le trafic réseau entrant acheminé vers votre instance. Le reste du trafic est ignoré. (Pour plus d'informations sur les groupes de sécurité, consultez [Groupes de sécurité Amazon EC2 pour vos instances EC2](#).) Sélectionnez ou créez un groupe de sécurité de la façon suivante, puis choisissez Vérifier et lancer.

- Pour sélectionner un groupe de sécurité existant, choisissez Select an existing security group (Sélectionner un groupe de sécurité existant), puis sélectionnez votre groupe de sécurité. Vous ne pouvez pas modifier les règles d'un groupe de sécurité existant, mais vous pouvez les copier dans un nouveau groupe en sélectionnant Copier vers le nouveau. Vous pouvez ensuite ajouter des règles, comme indiqué à l'étape suivante.
- Pour créer un nouveau groupe de sécurité, sélectionnez Create a new security group (Créer un nouveau groupe de sécurité). L'assistant définit automatiquement le groupe de sécurité launch-wizard-x et crée une règle entrante pour vous permettre de vous connecter à votre instance. Les instances Linux utilisent une règle entrante pour SSH (port 22) et les instances Windows utilisent une règle entrante pour RDP (port 3389).
- Vous pouvez ajouter des règles en fonction de vos besoins. Par exemple, si votre instance est un serveur web, ouvrez les ports 80 (HTTP) et 443 (HTTPS) afin d'autoriser le trafic Internet.

Pour ajouter une règle, choisissez Ajouter une règle, sélectionnez le protocole à ouvrir au trafic réseau, puis spécifiez la source. Sélectionnez Mon IP dans la liste Source afin de laisser l'assistant ajouter votre adresse IP publique à l'ordinateur. Toutefois, si votre connexion s'effectue via un ISP ou derrière un pare-feu sans adresse IP statique, vous devez déterminer la plage d'adresses IP utilisée par les ordinateurs clients.

 Warning

Les règles qui permettent à toutes les adresses IP (0.0.0.0/0) d'accéder à votre instance via SSH ou RDP sont acceptables dans le cadre de cet court exercice, mais pas assez sécurisées pour un environnement de production. Veillez à autoriser une seule adresse IP ou plage d'adresses à accéder à votre instance.

Étape 7 : Vérifier le lancement de l'instance et sélectionner une paire de clés

Sur la page Examiner le lancement de l'instance, vérifiez les détails de votre instance, puis effectuez les modifications nécessaires en sélectionnant le lien Modifier approprié.

Une fois que vous êtes prêt, choisissez Lancer.

Dans la boîte de dialogue Select an existing key pair or create a new key pair (Sélectionner une paire de clés existante ou créer une nouvelle paire de clés), vous pouvez choisir une paire de clés existante ou en créer une nouvelle. Par exemple, sélectionnez Choisir une paire de clés existante, puis choisissez la paire de clés que vous avez créée lors de la configuration. Pour plus d'informations, consultez [Paires de clés Amazon EC2 et instances Amazon EC2](#).

 Important

Si vous sélectionnez l'option Proceed without key pair (Continuer sans paire de clé), vous ne pourrez pas vous connecter à l'instance à moins de choisir une AMI configurée de façon à autoriser les utilisateurs à se connecter d'une autre façon.

Pour lancer votre instance, activez la case à cocher de confirmation, puis choisissez Lancer des instances.

(Facultatif) Vous pouvez créer une alarme de contrôle de statut pour l'instance (des frais supplémentaires peuvent être appliqués). Sur l'écran de confirmation, choisissez Créer des alarmes

de contrôle de statut et suivez les instructions. Des alarmes de vérification de statut peuvent également être créées après le lancement de l'instance. Pour plus d'informations, consultez [Créer et modifier des alarmes de vérification de statut](#).

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez [Résoudre les problèmes de lancement d'instance](#).

Lancer une instance à partir d'un modèle de lancement

Vous pouvez utiliser un modèle de lancement pour stocker les paramètres de lancement d'une instance afin de ne pas avoir à les spécifier chaque fois que vous lancez une instance. Par exemple, vous pouvez créer un modèle de lancement avec l'ID d'AMI, le type d'instance et les paramètres réseau que vous utilisez généralement pour lancer des instances. Lorsque vous lancez une instance à l'aide de la console Amazon EC2, d'un AWS SDK ou d'un outil de ligne de commande, vous pouvez spécifier le modèle de lancement au lieu de saisir à nouveau les paramètres.

Pour chaque modèle de lancement, vous pouvez créer une ou plusieurs versions de modèle de lancement numérotées. Chaque version peut comporter différents paramètres de lancement. Lorsque vous lancez une instance à partir d'un modèle de lancement, vous pouvez utiliser une version quelconque du modèle de lancement. Si vous ne spécifiez pas une version, c'est la version par défaut qui est utilisée. Vous pouvez définir n'importe quelle version du modèle de lancement comme version par défaut. Par défaut, il s'agit de la première version du modèle de lancement.

Le schéma suivant présente trois versions d'un modèle de lancement. La première version spécifie le type d'instance, l'ID d'AMI, le sous-réseau et la paire de clés à utiliser pour lancer l'instance. La deuxième version est basée sur la première et spécifie également un groupe de sécurité pour l'instance. La troisième version utilise différentes valeurs pour certains des paramètres. La version 2 est définie comme version par défaut. Si vous avez lancé une instance à partir de ce modèle de lancement, les paramètres de lancement de la version 2 sont utilisés si aucune autre version n'a été spécifiée.

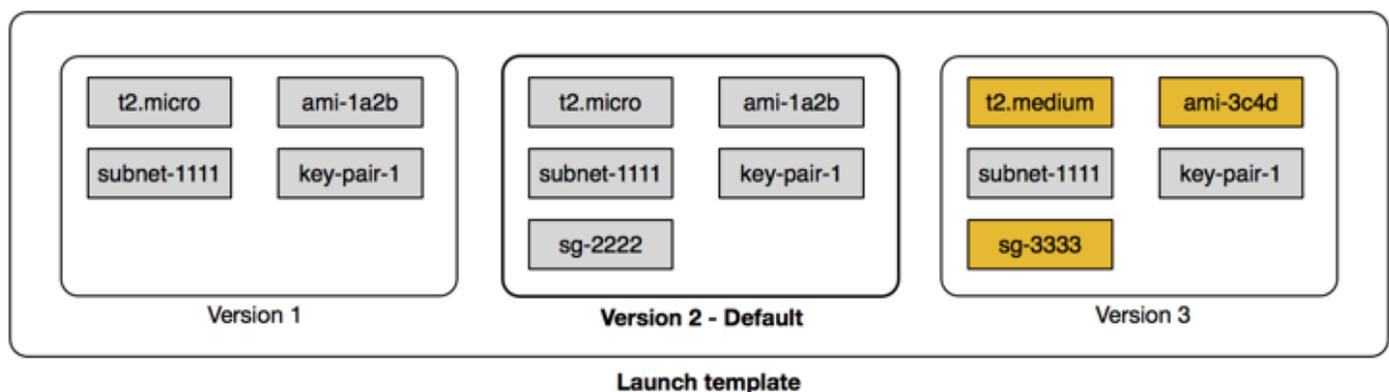


Table des matières

- [Restrictions du modèle de lancement](#)
- [Contrôlez l'accès aux modèles de lancement avec les autorisations IAM](#)
- [Utilisation de modèles de lancement pour contrôler le lancement d'instances](#)
- [Création d'un modèle de lancement](#)
- [Modifier un modèle de lancement \(gérer les versions du modèle de lancement\)](#)
- [Supprimer un modèle de lancement](#)
- [Lancer des instances à partir d'un modèle de lancement](#)

Restrictions du modèle de lancement

Les règles suivantes s'appliquent aux modèles de lancement et à leurs versions :

- **Quotas** : pour consulter les quotas de vos modèles de lancement et des versions de vos modèles de lancement, ouvrez la console [Service Quotas](#) ou utilisez la [list-service-quotas](#) AWS CLI commande. Chaque AWS compte peut avoir jusqu'à 5 000 modèles de lancement par région et jusqu'à 10 000 versions par modèle de lancement. Vos comptes peuvent avoir des quotas différents en fonction de leur ancienneté et de leur historique d'utilisation.
- **Les paramètres sont facultatifs** : les paramètres du modèle de lancement sont facultatifs. Néanmoins, vous devez vous assurer que votre demande de lancement d'une instance inclut tous les paramètres obligatoires. Par exemple, si votre modèle de lancement n'inclut pas un ID d'AMI, vous devez le spécifier avec un ID d'AMI lorsque vous lancez une instance.
- **Les paramètres ne sont pas validés** : les paramètres du modèle de lancement ne sont pas entièrement validés lorsque vous créez le modèle de lancement. Si vous spécifiez des valeurs incorrectes pour les paramètres ou si vous n'utilisez pas de combinaisons de paramètres prises en charge, aucune instance ne peut se lancer à l'aide de ce modèle de lancement. Veillez à spécifier les valeurs correctes des paramètres et à utiliser des combinaisons de paramètres prises en charge. Par exemple, pour lancer une instance dans un groupe de placement, vous devez spécifier un type d'instance pris en charge.
- **Balises** : vous pouvez baliser un modèle de lancement, mais pas une version de modèle de lancement.
- **Immutable** : les modèles de lancement sont immuables. Pour modifier un modèle de lancement, vous devez créer une nouvelle version du modèle de lancement.

- Numéros de version : les versions de modèles de lancement sont numérotées dans l'ordre de leur création. Après avoir créé une version de modèle de lancement, vous ne pouvez pas spécifier vous-même le numéro de version.

Contrôlez l'accès aux modèles de lancement avec les autorisations IAM

Vous pouvez utiliser les autorisations IAM pour contrôler les actions que les utilisateurs peuvent effectuer sur les modèles de lancement, telles que l'affichage, la création ou la suppression de modèles de lancement.

Lorsque vous autorisez les utilisateurs à créer des modèles de lancement et des versions de modèles de lancement, vous ne pouvez pas utiliser les autorisations au niveau des ressources pour restreindre les ressources qu'ils peuvent spécifier dans un modèle de lancement. Par conséquent, veillez à n'accorder les autorisations de création de modèles de lancement et de versions de modèles de lancement qu'aux administrateurs appropriés.

Vous devez accorder à toute personne qui utilisera un modèle de lancement les autorisations nécessaires pour créer et accéder aux ressources spécifiées dans le modèle de lancement. Par exemple :

- Pour lancer une instance à partir d'une Amazon Machine Image (AMI) privée partagée, l'utilisateur doit disposer d'une autorisation de lancement pour l'AMI.
- Pour créer des volumes EBS avec des balises provenant d'instantanés existants, l'utilisateur doit disposer d'un accès en lecture aux instantanés et des autorisations nécessaires pour créer et étiqueter des volumes.

Table des matières

- [ec2 : Modèle CreateLaunch](#)
- [ec2 : Modèles DescribeLaunch](#)
- [EC2 : DescribeLaunch TemplateVersions](#)
- [ec2 : Modèle DeleteLaunch](#)
- [Contrôler les autorisations de gestion des versions](#)
- [Contrôler l'accès aux balises sur les modèles de lancement](#)

ec2 : Modèle CreateLaunch

Pour créer un modèle de lancement dans la console ou à l'aide des API, le principal doit disposer de l'autorisation `ec2:CreateLaunchTemplate` dans une politique IAM. Dans la mesure du possible, utilisez des balises pour contrôler l'accès aux modèles de lancement de votre compte.

Par exemple, la déclaration de politique IAM suivante donne au principal l'autorisation de créer des modèles de lancement uniquement si le modèle utilise la balise spécifiée (*purpose=testing*).

```
{
  "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
  "Action": "ec2:CreateLaunchTemplate",
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/purpose": "testing"
    }
  }
}
```

Les principaux qui créent des clés peuvent avoir besoin de certaines autorisations associées, telles que :

- `ec2 : CreateTags` — Pour ajouter des balises au modèle de lancement pendant l'opération `CreateLaunchTemplate`, l'appelant doit avoir l'autorisation `ec2:CreateTags` requise dans une politique IAM.
- `ec2 : RunInstances` — Pour lancer des instances EC2 à partir du modèle de lancement qu'elles ont créé, le principal doit également disposer de l'autorisation `ec2:RunInstances` prévue dans une politique IAM.

Pour les actions de création de ressources qui appliquent des balises, les utilisateurs doivent être autorisés à effectuer l'action `ec2:CreateTags`. L'instruction de politique IAM suivante utilise la clé de condition `ec2:CreateAction` pour permettre aux utilisateurs de créer des balises uniquement dans le contexte de `CreateLaunchTemplate`. Les utilisateurs ne peuvent pas étiqueter les modèles de lancement existants ou d'autres ressources. Pour plus d'informations, consultez [Accorder l'autorisation de baliser les ressources lors de la création](#).

```
{
```

```
"Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
"Action": "ec2:CreateTags",
"Effect": "Allow",
"Resource": "arn:aws:ec2:region:account-id:launch-template/*",
"Condition": {
  "StringEquals": {
    "ec2:CreateAction": "CreateLaunchTemplate"
  }
}
```

L'utilisateur IAM qui crée un modèle de lancement n'est pas automatiquement autorisé à utiliser le modèle de lancement qu'il a créé. Comme tout autre principal, le créateur du modèle de lancement doit obtenir une autorisation par le biais d'une politique IAM. Si un utilisateur IAM souhaite lancer une instance EC2 à partir d'un modèle de lancement, il doit disposer de l'autorisation `ec2:RunInstances`. Lorsque vous accordez ces autorisations, vous pouvez spécifier que les utilisateurs ne peuvent utiliser que des modèles de lancement dotés de balises ou d'identifiants spécifiques. Vous pouvez également contrôler l'AMI et les autres ressources auxquelles toute personne utilisant des modèles de lancement peut faire référence et utiliser lors du lancement d'instances en spécifiant des autorisations au niveau des ressources pour l'appel à `RunInstances`. Pour obtenir des exemples de politiques, consultez [Modèles de lancement](#).

ec2 : Modèles DescribeLaunch

Pour répertorier les modèles de lancement dans le compte, le principal doit avoir l'autorisation `ec2:DescribeLaunchTemplates` dans une politique IAM. Parce que les actions `Describe` ne prennent pas en charge les autorisations au niveau des ressources, vous devez les spécifier sans condition et la valeur de l'élément de ressource dans la politique doit être `"*"`.

Par exemple, l'instruction de politique IAM suivante donne au principal l'autorisation de dresser la liste de tous les modèles de lancement du compte.

```
{
  "Sid": "IAMPolicyForDescribingLaunchTemplates",
  "Action": "ec2:DescribeLaunchTemplates",
  "Effect": "Allow",
  "Resource": "*"
}
```

EC2 : DescribeLaunch TemplateVersions

Les principaux qui consultent les modèles de lancement doivent également disposer de l'autorisation `ec2:DescribeLaunchTemplateVersions` de récupérer l'ensemble complet des attributs qui constituent les modèles de lancement.

Pour répertorier les versions de modèles de lancement dans le compte, le principal doit avoir l'autorisation `ec2:DescribeLaunchTemplateVersions` dans une politique IAM. Parce que les actions `Describe` ne prennent pas en charge les autorisations au niveau des ressources, vous devez les spécifier sans condition et la valeur de l'élément de ressource dans la politique doit être `"*"`.

Par exemple, l'instruction de politique IAM suivante donne au principal l'autorisation de dresser la liste de toutes les versions de modèles de lancement dans le compte.

```
{
  "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
  "Effect": "Allow",
  "Action": "ec2:DescribeLaunchTemplateVersions",
  "Resource": "*"
}
```

ec2 : Modèle DeleteLaunch

Important

Soyez prudent lorsque vous donnez aux principaux l'autorisation de supprimer une ressource. La suppression d'un modèle de lancement peut entraîner une défaillance d'une AWS ressource qui repose sur le modèle de lancement.

Pour supprimer un modèle de lancement, le principal doit avoir l'autorisation `ec2:DeleteLaunchTemplate` dans une politique IAM. Dans la mesure du possible, utilisez des clés de condition basées sur des balises pour limiter les autorisations.

Par exemple, l'instruction de politique IAM suivante donne au principal l'autorisation de supprimer des modèles de lancement uniquement si le modèle utilise la balise spécifiée (*purpose=testing*).

```
{
  "Sid": "IAMPolicyForDeletingLaunchTemplates",
  "Action": "ec2:DeleteLaunchTemplate",
```

```
"Effect": "Allow",
"Resource": "*",
"Condition": {
  "StringEquals": {
    "aws:ResourceTag/purpose": "testing"
  }
}
```

Vous pouvez également utiliser les ARN pour identifier le modèle de lancement auquel s'applique la politique IAM.

Un modèle de lancement possède l'ARN suivant.

```
"Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d310e"
```

Vous pouvez spécifier plusieurs ARN en les insérant dans une liste, ou vous pouvez spécifier une valeur Resource de "*" sans l'élément Condition permettant au principal de supprimer tout modèle de lancement du compte.

Contrôler les autorisations de gestion des versions

Pour les administrateurs de confiance, vous pouvez accorder l'accès à la création et à la suppression des versions d'un modèle de lancement, ainsi qu'à la modification de la version par défaut d'un modèle de lancement, en utilisant des politiques IAM similaires aux exemples suivants.

Important

Soyez prudent lorsque vous autorisez les principaux à créer des versions de modèles de lancement ou à modifier des modèles de lancement.

- Lorsque vous créez une version de modèle de lancement, vous affectez toutes les AWS ressources qui permettent à Amazon EC2 de lancer des instances en votre nom avec cette version. Latest
- Lorsque vous modifiez un modèle de lancement, vous pouvez changer de version Default et, par conséquent, affecter les AWS ressources qui permettent à Amazon EC2 de lancer des instances en votre nom avec cette version modifiée.

Vous devez également faire preuve de prudence dans la manière dont vous gérez les AWS ressources qui interagissent avec la version modèle Latest ou qui Default lancent une

version, telles que EC2 Fleet et Spot Fleet. Lorsqu'une version différente du modèle de lancement est utilisée en pour Latest ou Default, Amazon EC2 ne revérifie pas les autorisations de l'utilisateur pour les actions à effectuer lors du lancement de nouvelles instances pour remplir la capacité cible de la flotte, car il n'y a pas d'interaction de l'utilisateur avec la ressource AWS. En accordant à un utilisateur l'autorisation d'appeler les API `CreateLaunchTemplateVersion` et `ModifyLaunchTemplate`, il se voit également accorder l'autorisation `iam:PassRole` s'il fait pointer la flotte vers une version différente du modèle de lancement qui contient un profil d'instance (un conteneur pour un rôle IAM). Cela signifie qu'un utilisateur peut potentiellement mettre à jour un modèle de lancement pour passer un rôle IAM à une instance même s'il n'a pas l'autorisation `iam:PassRole`. Vous pouvez gérer ce risque en faisant preuve de prudence lorsque vous accordez des autorisations aux personnes habilitées à créer et à gérer les versions des modèles de lancement.

EC2 : CreateLaunchTemplateVersion

Pour créer une nouvelle version d'un modèle de lancement, le principal doit disposer de l'autorisation `ec2:CreateLaunchTemplateVersion` pour le modèle de lancement dans une politique IAM.

Par exemple, l'instruction de politique IAM suivante donne au principal l'autorisation de créer des versions de modèles de lancement uniquement si la version utilise la balise spécifiée (*`environment=production`*). Vous pouvez également spécifier un ou plusieurs ARN de modèles de lancement, ou vous pouvez spécifier une valeur `Resource` de "*" sans l'élément `Condition` permettant au principal de créer des versions de n'importe quel modèle de lancement dans le compte.

```
{
  "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
  "Action": "ec2:CreateLaunchTemplateVersion",
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/environment": "production"
    }
  }
}
```

EC2 : DeleteLaunchTemplateVersion

Important

Comme toujours, vous devez faire preuve de prudence lorsque vous autorisez les principaux à supprimer une ressource. La suppression d'une version du modèle de lancement peut entraîner une défaillance d'une AWS ressource qui repose sur la version du modèle de lancement.

Pour supprimer une version d'un modèle de lancement, le principal doit avoir l'autorisation `ec2:DeleteLaunchTemplateVersion` pour le modèle de lancement dans une politique IAM.

Par exemple, l'instruction IAM suivante donne au principal l'autorisation de supprimer des versions de modèles de lancement uniquement si la version utilise la balise spécifiée (*`environment=production`*). Vous pouvez également spécifier un ou plusieurs ARN de modèles de lancement, ou vous pouvez spécifier une valeur `Resource` de "*" sans l'élément `Condition` permettant au principal de supprimer les versions de n'importe quel modèle de lancement du compte.

```
{
  "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
  "Action": "ec2:DeleteLaunchTemplateVersion",
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/environment": "production"
    }
  }
}
```

EC2 : ModifyLaunchTemplate

Pour modifier la version `Default` associée à un modèle de lancement, le principal doit avoir l'autorisation `ec2:ModifyLaunchTemplate` pour le modèle de lancement dans une politique IAM.

Par exemple, l'instruction de politique IAM suivante donne au principal l'autorisation de modifier les modèles de lancement uniquement si le modèle de lancement utilise la balise spécifiée (*`environment=production`*). Vous pouvez également spécifier un ou plusieurs ARN de modèles

de lancement, ou vous pouvez spécifier une valeur Resource de "*" sans l'élément Condition permettant au principal de modifier n'importe quel modèle de lancement du compte.

```
{
  "Sid": "IAMPolicyForModifyingLaunchTemplates",
  "Action": "ec2:ModifyLaunchTemplate",
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/environment": "production"
    }
  }
}
```

Contrôler l'accès aux balises sur les modèles de lancement

Vous pouvez utiliser des clés de condition pour limiter les autorisations d'étiquetage lorsque la ressource est un modèle de lancement. Par exemple, la politique IAM suivante permet de ne supprimer que la balise avec la clé *temporary* dans les modèles de lancement dans le compte et la région spécifiés.

```
{
  "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
  "Action": "ec2:DeleteTags",
  "Effect": "Allow",
  "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "aws:TagKeys": [temporary]
    }
  }
}
```

Pour plus d'informations sur les clés de conditions que vous pouvez utiliser pour contrôler les clés de balise et les valeurs qui peuvent être appliquées aux ressources Amazon EC2, consultez [Contrôler l'accès à des balises spécifiques](#).

Utilisation de modèles de lancement pour contrôler le lancement d'instances

Vous pouvez spécifier que les utilisateurs peuvent uniquement lancer des instances s'il utilisent un modèle de lancement et qu'ils peuvent uniquement utiliser un modèle de lancement spécifique. Vous

pouvez également contrôler qui peut créer, modifier, décrire et supprimer les modèles de lancement et les versions du modèle de lancement.

Utiliser des modèles de lancement pour contrôler les paramètres de lancement

Un modèle de lancement peut contenir tout ou partie des paramètres permettant de lancer une instance. Lorsque vous lancez une instance à l'aide d'un modèle de lancement, vous pouvez remplacer les paramètres spécifiés dans le modèle de lancement. Vous pouvez également spécifier d'autres paramètres qui ne figurent pas dans le modèle de lancement.

Note

Vous ne pouvez pas supprimer les paramètres du modèle de lancement pendant le lancement (par exemple, vous ne pouvez pas spécifier une valeur nulle pour le paramètre). Pour supprimer un paramètre, créez une nouvelle version du modèle de lancement sans ce paramètre, puis utilisez cette version pour lancer l'instance.

Pour lancer des instances, les utilisateurs doivent avoir l'autorisation d'utiliser l'action `ec2:RunInstances`. Les utilisateurs doivent également être autorisés à créer ou à utiliser les ressources créées ou associées à l'instance. Vous pouvez utiliser des autorisations au niveau des ressources pour l'action `ec2:RunInstances` afin de contrôler les paramètres de lancement pouvant être spécifiés par les utilisateurs. Vous pouvez également autoriser les utilisateurs à lancer une instance à l'aide d'un modèle de lancement. Cela vous permet de gérer les paramètres de lancement dans un modèle de lancement plutôt que dans une politique IAM et d'utiliser un modèle de lancement comment moyen d'autoriser le lancement d'instances. Par exemple, vous pouvez spécifier que les utilisateurs peuvent uniquement lancer des instances à l'aide d'un modèle de lancement et qu'ils peuvent uniquement utiliser un modèle de lancement spécifique. Vous pouvez également contrôler les paramètres de lancement que les utilisateurs peuvent remplacer dans le modèle de lancement. Pour obtenir des exemples de politiques, consultez [Modèles de lancement](#).

Contrôler l'utilisation des modèles de lancement

Par défaut, les utilisateurs d' ne sont pas autorisés à utiliser des modèles de lancement. Vous pouvez créer une stratégie qui autorise les utilisateurs à créer, modifier, décrire et supprimer des modèles de lancement et leurs versions. Vous pouvez également appliquer des autorisations au niveau des ressources à certaines actions de modèle de lancement pour contrôler la capacité d'un utilisateur à utiliser des ressources spécifiques pour ces actions. Pour plus d'informations, consultez [Exemple : Utiliser des modèles de lancement](#).

Soyez vigilant lorsque vous autorisez des utilisateurs à effectuer les actions `ec2:CreateLaunchTemplate` et `ec2:CreateLaunchTemplateVersion`. Vous ne pouvez pas utiliser les autorisations au niveau des ressources pour contrôler les ressources que les utilisateurs peuvent spécifier dans le modèle de lancement. Pour limiter les ressources utilisées pour lancer une instance, veillez à autoriser uniquement les administrateurs appropriés à créer des modèles de lancement et des versions de modèles de lancement.

Problèmes de sécurité importants lors de l'utilisation de modèles de lancement avec la flotte d'EC2 ou le parc d'instances Spot

Pour utiliser les modèles de lancement, vous devez accorder à vos utilisateurs des autorisations pour créer, modifier, décrire et supprimer des modèles de lancement et leurs versions. Vous pouvez contrôler qui peut créer des modèles de lancement et des versions de modèles en contrôlant l'accès aux actions `ec2:CreateLaunchTemplate` et `ec2:CreateLaunchTemplateVersion`. Vous pouvez également contrôler qui peut modifier les modèles de lancement en contrôlant l'accès à l'action `ec2:ModifyLaunchTemplate`.

Important

Si une flotte d'EC2 ou un parc d'instances Spot est configuré pour utiliser la version de modèle de lancement « Dernière » ou « Par défaut », la flotte ou le parc n'est pas au courant si « Dernière » ou « Par défaut » sont modifiés ultérieurement pour pointer vers une version de modèle de lancement différente. Lorsqu'une version de modèle de lancement différente est utilisée pour « Dernière » ou « Par défaut », Amazon EC2 ne revérifie pas les autorisations pour les actions à effectuer lors du lancement de nouvelles instances afin de remplir la capacité cible de la flotte. Il s'agit d'une considération importante lorsque vous accordez des autorisations aux personnes qui peuvent créer et gérer des versions de modèles de lancement, en particulier l'action `ec2:ModifyLaunchTemplate` qui permet à un utilisateur de modifier la version de modèle de lancement « Par défaut ».

En accordant à un utilisateur l'autorisation d'utiliser les actions EC2 pour les API de modèles de lancement, il se voit également accorder l'autorisation `iam:PassRole` s'il crée ou met à jour une flotte d'EC2 ou un parc d'instances Spot pour pointer vers une version de modèle de lancement différente qui contient un profil d'instance (un conteneur pour un rôle IAM). Cela signifie qu'un utilisateur peut potentiellement mettre à jour un modèle de lancement pour passer un rôle IAM à une instance même s'il n'a pas l'autorisation `iam:PassRole`. Pour plus d'informations et un exemple de

politique IAM, consultez [Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations, consultez [Contrôler l'utilisation des modèles de lancement](#) et [Exemple : Utiliser des modèles de lancement](#).

Création d'un modèle de lancement

Créez un modèle de lancement à l'aide des paramètres que vous définissez, ou utilisez un modèle de lancement ou une instance existant comme base pour un nouveau modèle de lancement.

Tâches

- [Création d'un modèle de lancement à partir de paramètres](#)
- [Créer un modèle de lancement à partir d'un modèle de lancement existant](#)
- [Créer un modèle de lancement à partir d'une instance](#)
- [Utilisation d'un paramètre Systems Manager au lieu d'un ID d'AMI](#)

Création d'un modèle de lancement à partir de paramètres

Pour créer un modèle de lancement, vous devez spécifier son nom et au moins un paramètre de configuration d'instance.

Directions de la console

Pour créer un modèle de lancement à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement, puis Créer un modèle de lancement.
3. Les paramètres du modèle de lancement sont regroupés. Pour plus de détails sur chaque groupe, consultez les sections ci-dessous.
4. Utilisez le panneau Résumé pour vérifier la configuration de votre modèle de lancement. Vous pouvez accéder à n'importe quelle section en choisissant son lien, puis en apportant les modifications nécessaires.
5. Lorsque vous êtes prêt à créer votre modèle de lancement, choisissez Create launch template (Créer un modèle de lancement).

Nom, description et identifications du modèle de lancement

1. Pour Nom du modèle de lancement, entrez un nom descriptif pour le modèle.
2. Pour Description de la version du modèle, fournissez une brève description de cette version du modèle de lancement.
3. Pour [étiqueter](#) le modèle de lancement à la création, développez Template tags (Identifications du modèle), choisissez Add tag (Ajouter une identification), puis saisissez une paire de clé et de valeur d'identification. Choisissez Add tag (Ajouter une identification) pour chaque étiquette supplémentaire.

Note

Pour étiqueter les ressources créées lors du lancement d'une instance, vous devez spécifier les identifications sous Resource tags (Identifications de ressource). Pour plus d'informations, consultez [Balises de ressources](#).

Images d'applications et de systèmes d'exploitation (Amazon Machine Image)

Une Amazon Machine Image (AMI) contient les informations requises pour créer une instance. Par exemple, une AMI peut contenir le logiciel requis pour agir en tant que serveur Web, tel que Linux, Apache et votre site Web.

Vous pouvez trouver une AMI appropriée en procédant comme suit. Avec chaque option de recherche d'AMI, choisissez Cancel (Annuler) (en haut à droite) pour revenir au modèle de lancement sans choisir une AMI.

Barre de recherche

Pour effectuer une recherche parmi toutes les AMI disponibles, saisissez un mot-clé dans la barre de recherche d'AMI, puis appuyez sur Entrée. Pour sélectionner une AMI, choisissez Select (Sélectionner).

Recents (Récentes)

Les AMI que vous avez récemment utilisées.

Choisissez Recently launched (Lancées récemment) ou Currently in use (Actuellement en cours d'utilisation), puis, à partir de Amazon Machine Image (AMI), sélectionnez une AMI.

Mes AMI

Les AMI privées que vous possédez ou qui ont été partagées avec vous.

Choisissez Owned by me (M'appartenant) ou Shared with me (Partagées avec moi), puis, à partir de Amazon Machine Image (AMI), sélectionnez une AMI.

Quick Start

Les AMI sont regroupées par système d'exploitation afin de vous aider à démarrer rapidement.

Sélectionnez d'abord le système d'exploitation dont vous avez besoin, puis dans Amazon Machine Image (AMI), sélectionnez une AMI. Pour sélectionner une AMI éligible pour l'offre gratuite, assurez-vous que l'AMI indique Free tier eligible (Éligible à l'offre gratuite).

Browse more AMIs (Parcourir plus d'AMI)

Choisissez Browse more AMIs (Parcourir plus d'AMI) pour parcourir le catalogue complet des AMI.

- Pour effectuer une recherche parmi toutes les AMI disponibles, saisissez un mot-clé dans la barre de recherche, puis appuyez sur Entrée.
- Pour rechercher une AMI à l'aide d'un paramètre Systems Manager, sélectionnez le bouton fléché à droite de la barre de recherche, puis choisissez Search by Systems Manager parameter (Rechercher par paramètre Systems Manager). Pour plus d'informations, consultez [Rechercher une AMI à l'aide d'un paramètre de Systems Manager](#).
- Pour spécifier un paramètre Systems Manager qui sera converti en AMI au moment du lancement d'une instance à partir du modèle de lancement, sélectionnez le bouton fléché à droite de la barre de recherche, puis choisissez Spécifier une valeur personnalisée/paramètre Systems Manager. Pour plus d'informations, consultez [Utilisation d'un paramètre Systems Manager au lieu d'un ID d'AMI](#).
- Pour effectuer une recherche par catégorie, choisissez Quickstart AMIs (AMI de démarrage rapide), My AMIs (Mes AMI), AMIs (AMI), AWS Marketplace ou Community AMIs (AMI de la communauté).

AWS Marketplace Il s'agit d'une boutique en ligne où vous pouvez acheter des logiciels qui fonctionnent sur AWS, y compris des AMI. Pour plus d'informations sur le lancement d'une instance depuis le AWS Marketplace, consultez [Lancer une AWS Marketplace instance](#). Dans les AMI de communauté, vous trouverez les AMI que les membres de AWS la communauté ont mises à la disposition des autres utilisateurs. les AMI détenues par Amazon ou par un partenaire Amazon vérifié sont certifiées Fournisseur vérifié.

- Pour filtrer la liste des AMI, cochez une ou plusieurs cases sous Refine results (Affiner les résultats) sur la gauche de l'écran. Les options de filtre sont différentes selon la catégorie de recherche sélectionnée.
- Vérifiez le Type de périphérique racine spécifié pour chaque AMI. Déterminez les types d'AMI dont vous avez besoin, ebs (basées sur Amazon EBS) ou instance-store (basées sur le stockage d'instances). Pour plus d'informations, consultez [Stockage pour le périphérique racine](#).
- Vérifiez le Type de virtualisation spécifié pour chaque AMI. Déterminez le type d'AMI dont vous avez besoin, hvm ou paravirtual. Par exemple, certains types d'instance requièrent HVM. Pour plus d'informations, consultez [Types de virtualisation AMI](#).
- Vérifiez le mode de démarrage répertorié pour chaque AMI. Notez quelles AMI utilisent le mode de démarrage dont vous avez besoin : legacy-bios, uefi ou uefi-preferred. Pour plus d'informations, consultez [Modes de démarrage Amazon EC2](#).
- Choisissez une AMI correspondant à vos besoins, puis choisissez Sélectionner.

Type d'instance

Le type d'instance définit la configuration matérielle et la taille de l'instance. Les types d'instance plus importants disposent de plus d'UC et de mémoire. Pour plus d'informations, consultez les types [d'instances Amazon EC2](#).

Pour Instance type (Type d'instance), vous pouvez soit sélectionner un type d'instance, soit spécifier des attributs d'instance et laisser Amazon EC2 identifier les types d'instance avec ces attributs.

Note

La spécification d'attributs d'instance est prise en charge uniquement lorsque vous utilisez des groupes Auto Scaling, une flotte EC2 et un parc d'instances Spot pour lancer des instances. Pour plus d'informations, consultez [Création d'un groupe Auto Scaling à l'aide de la sélection de type d'instance basée sur des attributs](#), [Sélection de type d'instance basée sur des attributs pour la flotte EC2](#) et [Sélection de type d'instance basée sur des attributs pour un parc d'instances Spot](#).

Si vous prévoyez d'utiliser le modèle de lancement dans l'[assistant de lancement d'instance](#) ou avec l'[RunInstancesAPI](#), vous devez sélectionner un type d'instance.

- **Type d'instance** : assurez-vous que le type d'instance est compatible avec l'AMI spécifiée. Pour plus d'informations, consultez [Types d'instances Amazon EC2](#).
- **Comparaison des types d'instances** : vous pouvez comparer différents types d'instances en fonction des attributs suivants : nombre de vCPU, architecture, quantité de mémoire (Go), quantité de stockage (Go), type de stockage et performance réseau.
- **Obtenir des conseils** : vous pouvez obtenir des conseils et des suggestions concernant les types d'instances depuis le sélecteur de type d'instance Amazon Q EC2. Pour plus d'informations, consultez [Obtention de recommandations sur le type d'instance pour une nouvelle charge de travail](#).
- **Avancé** : pour spécifier des attributs d'instance et permettre à Amazon EC2 d'identifier les types d'instance avec ces attributs, choisissez Advanced (Avancé), puis Specify instance type attributes (Spécifier les attributs de type d'instance).
 - **Nombre de vCPU** : saisissez le nombre minimum et maximum de vCPU pour vos besoins de calcul. Pour n'indiquer aucune limite, saisissez un minimum de 0 et laissez le champ maximum vide.
 - **Quantité de mémoire (MiB)** : saisissez la quantité minimale et maximale de mémoire, en MiB, pour vos besoins en calcul. Pour n'indiquer aucune limite, saisissez un minimum de 0 et laissez le champ maximum vide.
 - **Développez Attributs de type d'instance facultatifs et choisissez Add attribute (Ajouter un attribut)** pour exprimer plus en détail vos besoins en matière de calcul. Pour plus d'informations sur chaque attribut, consultez [InstanceRequirementsRequest](#) dans le manuel Amazon EC2 API Reference.
 - **Resulting instance types (Types d'instance obtenus)** : vous pouvez prévisualiser les types d'instance qui correspondent aux attributs spécifiés. Pour exclure des types d'instance, choisissez Add attribute (Ajouter un attribut), et depuis la liste Attribute (Attribut), choisissez Excluded instance types (Types d'instance exclus). À partir de la liste Attribute value (Valeur d'attribut), sélectionnez les types d'instances à exclure.

Paire de clés (connexion)

La paire de clé correspondante à l'instance.

Pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou choisissez Create new key pair (Créer une nouvelle paire de clés) pour en créer une nouvelle. Pour plus d'informations, consultez [Paires de clés Amazon EC2 et instances Amazon EC2](#).

Paramètres réseau

Configurez les paramètres réseau, le cas échéant.

- **Sous-réseau** : vous pouvez lancer une instance dans un sous-réseau associé à une zone de disponibilité, une zone locale, une zone Wavelength ou un Outpost.

Pour lancer l'instance dans une zone de disponibilité, sélectionnez le sous-réseau dans lequel lancer votre instance. Pour créer un sous-réseau, choisissez Créer un nouveau sous-réseau afin d'accéder à la console Amazon VPC. Une fois que vous avez terminé, revenez dans l'assistant et choisissez l'icône Refresh (Actualiser) afin de charger votre sous-réseau dans la liste.

Pour lancer l'instance dans une zone locale, sélectionnez un sous-réseau que vous avez créé dans la zone locale.

Pour lancer une instance dans un Outpost, sélectionnez un sous-réseau dans un VPC que vous avez associé à l'Outpost.

- **Firewall (security groups) (Pare-feu (groupes de sécurité))** : utilisez un ou plusieurs groupes de sécurité afin de définir les règles de pare-feu de votre instance. Ces règles déterminent le trafic réseau entrant acheminé vers votre instance. Le reste du trafic est ignoré. Pour plus d'informations sur les groupes de sécurité, consultez [Groupes de sécurité Amazon EC2 pour vos instances EC2](#).

Si vous ajoutez une interface réseau, vous devez indiquer les mêmes groupes de sécurité dans l'interface réseau.

Sélectionnez ou créez un groupe de sécurité de la façon suivante :

- Pour sélectionner un groupe de sécurité existant, choisissez Select existing security group (Sélectionner un groupe de sécurité existant), puis sélectionnez votre groupe de sécurité dans Common security groups (Groupes de sécurité courants).
- Pour créer un nouveau groupe de sécurité, sélectionnez Create security group (Créer un groupe de sécurité).

Vous pouvez ajouter des règles en fonction de vos besoins. Par exemple, si votre instance sera un serveur web, ouvrez les ports 80 (HTTP) et 443 (HTTPS) afin d'autoriser le trafic Internet.

Pour ajouter une règle, choisissez Add security group rule (Ajouter une règle de groupe de sécurité). Pour Type, sélectionnez le type de trafic réseau. Le champ Protocol (Protocole) est automatiquement rempli avec le protocole pour s'ouvrir au trafic réseau. Pour Source type (Type de source), sélectionnez le type de source. Sélectionnez My IP (Mon IP) afin de permettre au

modèle de lancement d'ajouter l'adresse IP publique de votre ordinateur. Toutefois, si votre connexion s'effectue via un ISP ou derrière un pare-feu sans adresse IP statique, vous devez déterminer la plage d'adresses IP utilisée par les ordinateurs clients.

 Warning

Les règles qui activent toutes les adresses IP ($0.0.0.0/0$) pour accéder à votre instance via SSH ou RDP sont acceptables si vous lancez brièvement une instance de test et que vous l'arrêtez ou la résiliez bientôt, mais ne sont pas acceptables pour un environnement de production. Veillez à autoriser une seule adresse IP ou plage d'adresses à accéder à votre instance.

- Advanced network configuration (Configuration de mise en réseau avancée)

Interface réseau

- Index du périphérique : numéro du périphérique correspondant à l'interface réseau, par exemple `eth0` pour l'interface réseau principale. Si vous ne renseignez pas ce champ, AWS crée l'interface réseau principale.
- Network interface (Interface réseau) : sélectionnez New interface (Nouvelle interface) pour permettre à Amazon EC2 de créer une nouvelle interface, ou sélectionnez une interface réseau disponible et existante.
- Description : (facultatif) description de la nouvelle interface réseau.
- Subnet (Sous-réseau) : sous-réseau dans lequel créer une nouvelle interface réseau. Pour l'interface réseau principale (`eth0`), il s'agit du sous-réseau dans lequel l'instance est lancée. Si vous avez indiqué une interface réseau existante pour `eth0`, l'instance est lancée dans le sous-réseau dans lequel l'interface réseau est située.
- Groupes de sécurité : un ou plusieurs groupes de sécurité de votre VPC auxquels associer l'interface réseau.
- Auto-assign public IP (Attribuer automatiquement l'adresse IP publique) : indiquez si l'instance est associée à une adresse IPv4 publique. Par défaut, les instances d'un sous-réseau par défaut se voient attribuer une adresse IPv4 publique, contrairement aux instances d'un sous-réseau personnalisé. Vous pouvez sélectionner Activer ou Désactiver pour remplacer la configuration par défaut du sous-réseau. Pour plus d'informations, consultez [Adresses IPv4 publiques](#).
- IP principale : une adresse IPv4 privée de la plage d'adresses de votre sous-réseau. Laissez ce champ vide pour qu'Amazon EC2 choisisse une adresse IPv4 privée à votre place.

- **Secondary IP (Adresse IP secondaire)** : une ou plusieurs adresses IPv4 privées supplémentaires de la plage d'adresses de votre sous-réseau. Choisissez **Manually assign (Attribuer manuellement)** et saisissez une adresse IP. Choisissez **Add IP (Ajouter une adresse IP)** pour ajouter une autre adresse IP. Sinon, choisissez **Automatically assign (Attribuer automatiquement)** pour laisser Amazon EC2 en choisir une pour vous et saisissez une valeur indiquant le nombre d'adresses IP à ajouter.
- **(IPv6 uniquement) Adresses IP IPv6** : adresse IPv6 comprise dans la plage du sous-réseau. Choisissez **Manually assign (Attribuer manuellement)** et saisissez une adresse IP. Choisissez **Add IP (Ajouter une adresse IP)** pour ajouter une autre adresse IP. Sinon, choisissez **Automatically assign (Attribuer automatiquement)** pour laisser Amazon EC2 en choisir une pour vous et saisissez une valeur indiquant le nombre d'adresses IP à ajouter.
- **Préfixes IPv4** : les préfixes IPv4 pour l'interface réseau.
- **Préfixes IPv6** : les préfixes IPv6 pour l'interface réseau.
- **(Facultatif) Attribuer une adresse IP IPv6 principale** : si vous lancez une instance sur un sous-réseau à double pile ou uniquement IPv6, vous avez la possibilité d'Attribuer une adresse IP IPv6 principale. L'attribution d'une adresse IPv6 principale vous permet d'éviter de perturber le trafic vers les instances ou les ENI. Choisissez **Activer** si cette instance dépend du fait que son adresse IPv6 ne change pas. Lorsque vous lancez l'instance, une adresse IPv6 associée à l'ENI attachée à votre instance AWS sera automatiquement attribuée comme adresse IPv6 principale. Une fois que vous avez activé une adresse GUA IPv6 comme adresse IPv6 principale, vous ne pouvez pas la désactiver. Lorsque vous activez une adresse GUA IPv6 comme adresse IPv6 principale, la première GUA IPv6 devient l'adresse IPv6 principale jusqu'à ce que l'instance soit résiliée ou que l'interface réseau soit détachée. Si plusieurs adresses IPv6 sont associées à une ENI attachée à votre instance et que vous activez une adresse IPv6 principale, la première adresse GUA IPv6 associée à l'ENI devient l'adresse IPv6 principale.
- **Supprimer à la résiliation** : indiquez s'il convient de supprimer l'interface réseau à la suppression de l'instance.
- **Elastic Fabric Adapter (EFA)** : Indique si l'interface réseau est une Elastic Fabric Adapter (EFA). Pour plus d'informations, consultez [the section called "Elastic Fabric Adapter"](#).
- **Index de carte réseau** : l'index de la carte réseau. L'interface réseau principale doit être affectée à l'index de carte réseau 0. Certains types d'instance prennent en charge plusieurs cartes réseau.
- **ENA Express** : ENA Express est alimenté par la technologie AWS Scalable Reliable Datagram (SRD). La technologie SRD utilise un mécanisme de pulvérisation de paquets pour répartir la charge et éviter la congestion du réseau. L'activation d'ENA Express permet aux instances

prises en charge de communiquer en utilisant le SRD en plus du trafic TCP normal lorsque cela est possible. Le modèle de lancement n'inclut pas la configuration ENA Express pour l'instance, sauf si vous sélectionnez Activer ou Désactiver.

- ENA Express UDP : si vous avez activé ENA Express, vous pouvez éventuellement l'utiliser pour le trafic UDP. Le modèle de lancement n'inclut pas la configuration ENA Express pour l'instance, sauf si vous sélectionnez Activer ou Désactiver.

Pour ajouter plusieurs interfaces réseau, choisissez Add network interface (Ajouter une interface réseau). Le nombre d'interfaces réseau que vous pouvez ajouter dépend du nombre pris en charge par le type d'instance sélectionné. Des interfaces réseau supplémentaires peuvent résider dans un sous-réseau différent du même VPC ou dans un sous-réseau d'un autre VPC que vous possédez (à condition que le sous-réseau se trouve dans la même zone de disponibilité que votre instance). Si vous sélectionnez un sous-réseau dans un autre VPC, l'étiquette Multi-VPC apparaît à côté de l'interface réseau que vous avez ajoutée. Cela vous permet de créer des instances multi-résidents entre des VPC dotés de différentes configurations réseau et de sécurité. Notez que si vous attachez une ENI supplémentaire depuis un autre VPC, vous devez choisir un groupe de sécurité pour l'ENI à partir de ce VPC.

Pour plus d'informations, consultez [Interfaces réseau Elastic](#). Si vous spécifiez plusieurs interfaces réseau, votre instance ne peut recevoir aucune adresse IPv4 publique. En outre, si vous spécifiez une interface réseau existante pour eth0, vous ne pouvez pas remplacer le paramètre d'adresse IPv4 publique du sous-réseau à l'aide de Attribuer automatiquement l'adresse IP publique. Pour plus d'informations, consultez [Attribuer une adresse IPv4 publique lors du lancement d'une instance](#).

Configurer le stockage

Si vous spécifiez une AMI pour le modèle de lancement, l'AMI inclut un ou plusieurs volumes de stockage, notamment le volume racine (Volume 1 (AMI Root)) (Volume 1 (racine AMI)). Vous pouvez spécifier d'autres volumes à attacher à l'instance.

Vous pouvez utiliser la vue Simple ou Advanced (Avancée). Avec la vue Simple, vous spécifiez la taille et le type de volume. Pour spécifier tous les paramètres de volume, choisissez la vue Advanced (Avancée) (en haut à droite de la carte).

Pour ajouter un nouveau volume, choisissez Ajouter un volume.

En utilisant la vue Advanced (Avancée), vous pouvez configurer chaque volume comme suit :

- **Storage type (Type de stockage)** : le type de volume (EBS ou éphémère) à associer à votre instance. Le type de volume de stockage d'instances (éphémère) est disponible uniquement si vous sélectionnez un type d'instance qui le prend en charge. Pour plus d'informations, consultez [Stockage d'instances Amazon EC2](#) et [volumes Amazon EBS](#).
- **Device name (Nom du dispositif)** : sélectionnez le périphérique dans la liste des noms de périphériques disponibles pour le volume.
- **Snapshot (Instantané)** : sélectionnez l'instantané à partir duquel vous souhaitez créer le volume. Vous pouvez rechercher les instantanés partagés et publics disponibles en saisissant un texte dans le champ Snapshot (Instantané).
- **Size (GiB) (Taille (Gio))** : pour les volumes EBS, vous pouvez spécifier une taille de stockage. Si vous avez sélectionné une AMI et une instance éligibles pour l'offre gratuite, n'oubliez pas que pour ne pas dépasser les limites de celle-ci, vous devez veiller à ne pas dépasser 30 GiO de stockage au total.
- **Volume type (Type de volume)** : pour les volumes EBS, sélectionnez un type de volume. Pour plus d'informations, consultez les [types de volumes Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.
- **IOPS** : si vous avez sélectionné un type de volume SSD d'IOPS provisionnés (io1 et io2) ou SSD polyvalents (gp3), alors vous pouvez saisir le nombre d'opérations d'I/O par seconde (IOPS) que le volume peut prendre en charge. Ceci est requis pour les volumes io1, io2 et gp3. Il n'est pas pris en charge pour les volumes gp2, st1, sc1 ou standard. Si vous omettez ce paramètre pour le modèle de lancement, vous devez lui spécifier une valeur lorsque vous lancez une instance à partir du modèle de lancement.
- **Delete on termination (Supprimer à la résiliation)** : pour les volumes Amazon EBS, choisissez Yes (Oui) afin de supprimer le volume lors de la résiliation de l'instance ou No (Non) afin de conserver le volume. Pour plus d'informations, consultez [Conservation des données lors de la résiliation d'une instance](#).
- **Encrypted (Chiffré)** : si le type d'instance prend en charge le chiffrement EBS, vous pouvez sélectionner Yes (Oui) pour activer le chiffrement du volume. Si vous avez activé le chiffrement par défaut dans cette région, le chiffrement est activé automatiquement. Pour plus d'informations, consultez la section relative au [chiffrement Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.
- **KMS Key (Clé KMS)** : si vous avez sélectionné Yes (Oui) pour Encrypted (Chiffré), vous devez ensuite sélectionner une clé gérée par le client à utiliser pour chiffrer le volume. Si vous avez activé le chiffrement par défaut dans cette région, la clé gérée par le client par défaut est sélectionnée.

pour vous. Vous pouvez sélectionner une clé différente ou spécifier l'ARN de n'importe quelle clé gérée par le client que vous avez créée.

Balises de ressources

Pour [étiqueter](#) les ressources créées lors du lancement d'une instance, sous Resource tags (Identifications de ressource), choisissez Add tag (Ajouter une identification), puis entrez une paire de clé et de valeur d'identification. Pour Resource types (Types de ressource), spécifiez les ressources à étiqueter lors de la création. Vous pouvez spécifier la même identification pour toutes les ressources ou spécifier des identifications différentes pour différentes ressources. Choisissez Add tag (Ajouter une identification) pour chaque étiquette supplémentaire.

Vous pouvez spécifier des identifications pour les ressources suivantes qui sont créées lorsqu'un modèle de lancement est utilisé :

- instances
- Volumes
- Demandes d'instance Spot
- Interfaces réseau

Note

Pour étiqueter le modèle de lancement lui-même, vous devez spécifier les identifications sous Template tags (Identifications de modèle). Pour plus d'informations, consultez [Nom, description et identifications du modèle de lancement](#).

Détails avancés

Développez la section Détails avancés pour afficher les champs et spécifier des paramètres supplémentaires pour l'instance.

- Purchasing option (Option d'achat) : choisissez Request Spot Instances (Demander des instances Spot) pour demander des instances Spot au prix Spot, plafonné au prix à la demande, et choisissez Customize (Personnaliser) pour modifier les paramètres par défaut de l'instance Spot. Vous pouvez définir votre prix maximum (non recommandé) et modifier le type de demande, la durée de la demande et le comportement d'interruption. Si vous ne demandez pas une instance

Spot, EC2 lance une instance à la demande par défaut. Pour plus d'informations, consultez [Spot instances](#).

- IAM instance profile (Profil d'instance IAM) : sélectionnez un profil d'instance AWS Identity and Access Management (IAM) à associer à l'instance. Pour plus d'informations, consultez [Rôles IAM pour Amazon EC2](#).
- Hostname type (Type de nom d'hôte) : sélectionnez si le nom d'hôte du système d'exploitation hôte de l'instance inclura le nom de la ressource ou le nom de l'adresse IP. Pour plus d'informations, consultez [Types de noms d'hôtes des instances Amazon EC2](#).
- DNS Hostname (Nom d'hôte DNS) : détermine si les requêtes DNS relatives au nom de la ressource ou au nom de l'adresse IP (selon votre choix pour Hostname type [Type de nom d'hôte]) répondront à l'aide de l'adresse IPv4 (registre A), de l'adresse IPv6 (registre AAAA), ou des deux. Pour plus d'informations, consultez [Types de noms d'hôtes des instances Amazon EC2](#).
- Comportement d'arrêt : indiquez si l'instance doit s'arrêter ou être résiliée lorsque vous arrêtez l'ordinateur. Pour plus d'informations, consultez [Modifier le comportement d'arrêt lancé de l'instance](#).
- Stop - Hibernate behavior (Comportement d'arrêt - mise en veille prolongée) : pour activer la mise en veille prolongée, sélectionnez Enable (Activer). Ce champ est valide uniquement pour les instances pour lesquelles les prérequis de mise en veille prolongée sont satisfaits. Pour plus d'informations, consultez [Hibernez votre instance Amazon EC2](#).
- Termination protection (Protection de la résiliation) : pour éviter toute mise hors service accidentelle, sélectionnez Enable (Activer). Pour plus d'informations, consultez [Activer la protection de la résiliation](#).
- Stop protection (Protection contre l'arrêt) : pour éviter tout arrêt accidentel, choisissez Enable (Activer). Pour plus d'informations, consultez [Activer la protection contre l'arrêt](#).
- CloudWatch Surveillance détaillée : choisissez Activer pour activer la surveillance détaillée de l'instance à l'aide d'Amazon CloudWatch. Des frais supplémentaires seront facturés. Pour plus d'informations, consultez [Surveillez vos instances à l'aide de CloudWatch](#).
- GPU élastique : Amazon Elastic Graphics a atteint la fin de son cycle de vie le 8 janvier 2024. Pour les charges de travail nécessitant une accélération graphique, nous vous recommandons d'utiliser des instances Amazon EC2 G4ad, G4dn ou G5.
- Elastic inference (Inférence Elastic) : accélérateur d'inférence Elastic à attacher à votre instance de CPU EC2. Pour plus d'informations, consultez [Utilisation d'Amazon Elastic Inference](#) dans le Guide du développeur Amazon Elastic Inference.

Note

À compter du 15 avril 2023, AWS nous n'intégrerons pas de nouveaux clients à Amazon Elastic Inference (EI) et nous aiderons les clients actuels à migrer leurs charges de travail vers des options offrant un meilleur prix et de meilleures performances. Après le 15 avril 2023, les nouveaux clients ne pourront plus lancer d'instances avec les accélérateurs Amazon EI sur Amazon SageMaker, Amazon ECS ou Amazon EC2. Toutefois, les clients qui ont utilisé Amazon EI au moins une fois au cours des 30 derniers jours sont considérés comme des clients actuels et pourront continuer à utiliser le service.

- **Credit specification (Spécification de crédit)** : sélectionnez Unlimited (Non limité) pour permettre aux applications de s'exécuter au-delà du niveau de référence aussi longtemps que nécessaire. Ce champ est valable uniquement pour les instances T. Des frais supplémentaires peuvent être facturés. Pour plus d'informations, consultez [Instance de performance à capacité extensible](#).
- **Nom du groupe de placement** : indiquez un groupe de placement dans lequel lancer l'instance. Vous pouvez sélectionner un groupe de placement existant ou en créer un nouveau. Le lancement dans un groupe de placement n'est pas possible pour tous les types d'instance. Pour plus d'informations, consultez [Groupes de placement](#).
- **EBS-optimized instance** : Sélectionnez Enable (Activer) pour fournir une capacité supplémentaire dédiée pour les I/O Amazon EBS. Cette fonction n'est pas prise en charge par tous les types d'instance. Des frais supplémentaires seront facturés. Pour plus d'informations, consultez [the section called "Optimisation EBS"](#).
- **Capacity Reservation (Réserve de capacité)** : indiquez s'il convient de lancer l'instance dans une réserve de capacité (Open (Ouvrir)), dans une réserve de capacité spécifique (Target by ID (Cibler par ID)) ou dans un groupe de réserve de capacité (Target by group (Cibler par groupe)). Pour spécifier qu'il ne faut pas utiliser de réserve de capacité, choisissez None (Aucune). Pour plus d'informations, consultez [Lancer des instances dans une Réserve de capacité existante](#).
- **Location** : indiquez s'il convient d'exécuter votre instance sur un matériel partagé (Partagé), isolé, dédié (Dédié) ou sur un Hôte dédié (Hôte dédié). Si vous choisissez de lancer l'instance sur un Hôte dédié, vous pouvez spécifier si l'instance doit être lancée dans un groupe de ressources hôte ou vous pouvez cibler un Hôte dédié spécifique. Des frais supplémentaires peuvent être facturés. Pour plus d'informations, consultez [Dedicated instances](#) et [Hôtes dédiés](#).
- **RAM disk ID (ID de disque RAM)** : (valide uniquement pour les AMI paravirtuelles (PV)) Sélectionnez un disque RAM pour l'instance. Si vous avez sélectionné un noyau, vous devrez peut-être sélectionner un disque RAM spécifique avec les pilotes qui l'accompagnent.

- Kernel ID (ID du noyau) : (valide uniquement pour les AMI paravirtuelles (PV)) Sélectionnez un noyau pour l'instance.
- Nitro Enclave : permet de créer des environnements d'exécution isolés, appelés enclaves, à partir d'instances Amazon EC2. Sélectionnez Enable (Activer) pour activer l'instance pour AWS Nitro Enclaves. Pour plus d'informations, voir [Qu'est-ce qu' AWS Nitro Enclaves ?](#) dans le Guide de l'utilisateur AWS Nitro Enclaves.
- Configurations de licence : vous pouvez lancer des instances sur la configuration de licence spécifiée pour suivre l'utilisation de votre licence. Pour plus d'informations, consultez [Create a License Configuration](#) (Création d'une configuration de licence) dans le Guide de l'utilisateur AWS License Manager.
- Specify CPU options (Spécifier les options d'UC) : choisissez Specify CPU options (Spécifier les options d'UC) pour spécifier un nombre personnalisé de vCPU lors du lancement. Définissez le nombre de cœurs d'UC et de threads par cœur. Pour plus d'informations, consultez [Optimiser les options d'UC](#).
- Point de terminaison IPv6 des métadonnées : vous pouvez autoriser l'instance à utiliser l'adresse IPv6 IMDS [fd00:ec2::254] pour récupérer les métadonnées de l'instance. Cette option n'est disponible que si vous lancez [des instances basées sur le système AWS Nitro](#) dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement). Pour plus d'informations, consultez [Récupérer des métadonnées d'instance](#).
- Métadonnées accessibles : vous pouvez activer ou désactiver l'accès à l'IMDS. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les nouvelles instances](#).
- Version des métadonnées : si vous activez l'accès à l'IMDS, vous pouvez choisir d'exiger l'utilisation du service des métadonnées d'instance Version 2 lors de la demande de métadonnées d'instance. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les nouvelles instances](#).
- Durée de vie de réponse des métadonnées : si vous activez l'IMDS, vous pouvez définir le nombre autorisé de sauts réseau pour le jeton de métadonnées. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les nouvelles instances](#).
- Allow tags in metadata (Autoriser les balises dans les métadonnées) : si vous sélectionnez Enable (Activer), l'instance autorise l'accès à toutes les balises de l'instance à partir de ses métadonnées. Si vous n'incluez pas ce paramètre dans le modèle, l'accès aux identifications dans les métadonnées d'instance est désactivé par défaut. Pour plus d'informations, consultez [Autoriser l'accès aux identifications dans les métadonnées d'instance](#).

- Données utilisateur : vous pouvez spécifier les données utilisateur pour configurer une instance lors du lancement ou pour exécuter un script de configuration. Pour plus d'informations, consultez [Exécutez des commandes sur votre instance Amazon EC2 au lancement](#).

AWS CLI exemple

L'exemple suivant utilise la commande [create-launch-template](#) pour créer un modèle de lancement avec le nom et la configuration d'instance spécifiés.

```
aws ec2 create-launch-template \  
  --launch-template-name TemplateForWebServer \  
  --version-description WebVersion1 \  
  --tag-specifications 'ResourceType=launch-  
template,Tags=[{Key=purpose,Value=production}]' \  
  --launch-template-data file://template-data.json
```

Voici un exemple de code JSON qui spécifie les données du modèle de lancement pour la configuration de l'instance. Enregistrez le JSON dans un fichier et incluez-le dans le `--launch-template-data` paramètre, comme indiqué dans l'exemple de commande.

```
{  
  "NetworkInterfaces": [{  
    "AssociatePublicIpAddress": true,  
    "DeviceIndex": 0,  
    "Ipv6AddressCount": 1,  
    "SubnetId": "subnet-7b16de0c"  
  }],  
  "ImageId": "ami-8c1be5f6",  
  "InstanceType": "r4.4xlarge",  
  "TagSpecifications": [{  
    "ResourceType": "instance",  
    "Tags": [{  
      "Key": "Name",  
      "Value": "webserver"  
    }]  
  }],  
  "CpuOptions": {  
    "CoreCount": 4,  
    "ThreadsPerCore": 2  
  }  
}
```

Voici un exemple de sortie.

```
{
  "LaunchTemplate": {
    "LatestVersionNumber": 1,
    "LaunchTemplateId": "lt-01238c059e3466abc",
    "LaunchTemplateName": "TemplateForWebServer",
    "DefaultVersionNumber": 1,
    "CreatedBy": "arn:aws:iam::123456789012:root",
    "CreateTime": "2017-11-27T09:13:24.000Z"
  }
}
```

AWS Tools for Windows PowerShell exemple

L'exemple suivant utilise l'[New-EC2LaunchTemplate](#) applet de commande pour créer un modèle de lancement avec le nom et la configuration d'instance spécifiés.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
  ImageId = 'ami-8c1be5f6'
  InstanceType = 'r4.4xlarge'
  NetworkInterfaces = @(
    [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
      AssociatePublicIpAddress = $true
      DeviceIndex = 0
      Ipv6AddressCount = 1
      SubnetId = 'subnet-7b16de0c'
    }
  )
  TagSpecifications = @(
    [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
      ResourceType = 'instance'
      Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'Name'
        Value = 'webserver'
      }
    }
  )
  CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
    CoreCount = 4
    ThreadsPerCore = 2
  }
}
```

```
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' -VersionDescription
'WebVersion1' -LaunchTemplateData $launchTemplateData -TagSpecification
$tagSpecificationData
```

Voici un exemple de sortie.

```
CreatedBy          : arn:aws:iam::123456789012:root
CreateTime         : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId    : lt-01238c059eEXAMPLE
LaunchTemplateName  : TemplateForWebServer
Tags                : {purpose}
```

Créer un modèle de lancement à partir d'un modèle de lancement existant

Vous pouvez cloner un modèle de lancement existant, puis ajuster les paramètres pour créer un modèle de lancement. Toutefois, vous ne pouvez le faire que lorsque vous utilisez la console Amazon EC2 ; le clonage d'un modèle AWS CLI n'est pas pris en charge.

Console

Pour créer un modèle de lancement à partir d'un modèle de lancement existant

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement, puis Créer un modèle de lancement.
3. Pour Nom du modèle de lancement, entrez un nom descriptif pour le modèle.
4. Pour Description de la version du modèle, fournissez une brève description de cette version du modèle de lancement.
5. Pour baliser le modèle de lancement à la création, développez Template tags (Balises du modèle), Ajouter la balise, puis entrez une paire de clé et de valeur de balise.

6. Développez Modèle source, et, pour Nom du modèle de lancement, choisissez un modèle de lancement sur lequel baser le nouveau modèle.
7. Pour Version du modèle source, choisissez la version du modèle de lancement sur laquelle baser le nouveau modèle de lancement.
8. Ajustez les paramètres de lancement si nécessaire, puis choisissez Créer un modèle de lancement.

Créer un modèle de lancement à partir d'une instance

Console

Pour créer un modèle de lancement à partir d'une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, Créer un modèle à partir d'une instance.
4. Indiquez un nom, une description et des balises, puis ajustez les paramètres de lancement si nécessaire.

Note

Lorsque vous créez un modèle de lancement à partir d'une instance, les ID et adresses IP de l'interface réseau de l'instance ne sont pas inclus dans le modèle.

5. Choisissez Créer un modèle de lancement.

AWS CLI

Vous pouvez utiliser le AWS CLI pour créer un modèle de lancement à partir d'une instance existante en obtenant d'abord les données du modèle de lancement à partir d'une instance, puis en créant un modèle de lancement à l'aide des données du modèle de lancement.

Pour obtenir des données de modèle de lancement à partir d'une instance

- Utilisez la commande [get-launch-template-data](#) et spécifiez l'ID d'instance. Vous pouvez utiliser la sortie comme base pour créer un modèle de lancement ou une version de modèle de lancement. Par défaut, la sortie contient un objet `LaunchTemplateData` de niveau

supérieur qui ne peut pas être spécifié dans les données de modèle de lancement. Excluez cet objet à l'aide de l'option `--query`.

```
aws ec2 get-launch-template-data \  
  --instance-id i-0123d646e8048babc \  
  --query "LaunchTemplateData"
```

Voici un exemple de sortie.

```
{  
  "Monitoring": {},  
  "ImageId": "ami-8c1be5f6",  
  "BlockDeviceMappings": [  
    {  
      "DeviceName": "/dev/xvda",  
      "Ebs": {  
        "DeleteOnTermination": true  
      }  
    }  
  ],  
  "EbsOptimized": false,  
  "Placement": {  
    "Tenancy": "default",  
    "GroupName": "",  
    "AvailabilityZone": "us-east-1a"  
  },  
  "InstanceType": "t2.micro",  
  "NetworkInterfaces": [  
    {  
      "Description": "",  
      "NetworkInterfaceId": "eni-35306abc",  
      "PrivateIpAddresses": [  
        {  
          "Primary": true,  
          "PrivateIpAddress": "10.0.0.72"  
        }  
      ],  
      "SubnetId": "subnet-7b16de0c",  
      "Groups": [  
        "sg-7c227019"  
      ],  
      "Ipv6Addresses": [  

```

```
        {
            "Ipv6Address": "2001:db8:1234:1a00::123"
        }
    ],
    "PrivateIpAddress": "10.0.0.72"
}
]
```

Par exemple, vous pouvez écrire directement la sortie dans un fichier :

```
aws ec2 get-launch-template-data \
  --instance-id i-0123d646e8048babc \
  --query "LaunchTemplateData" >> instance-data.json
```

Pour créer un modèle de lancement à l'aide des données du modèle de lancement

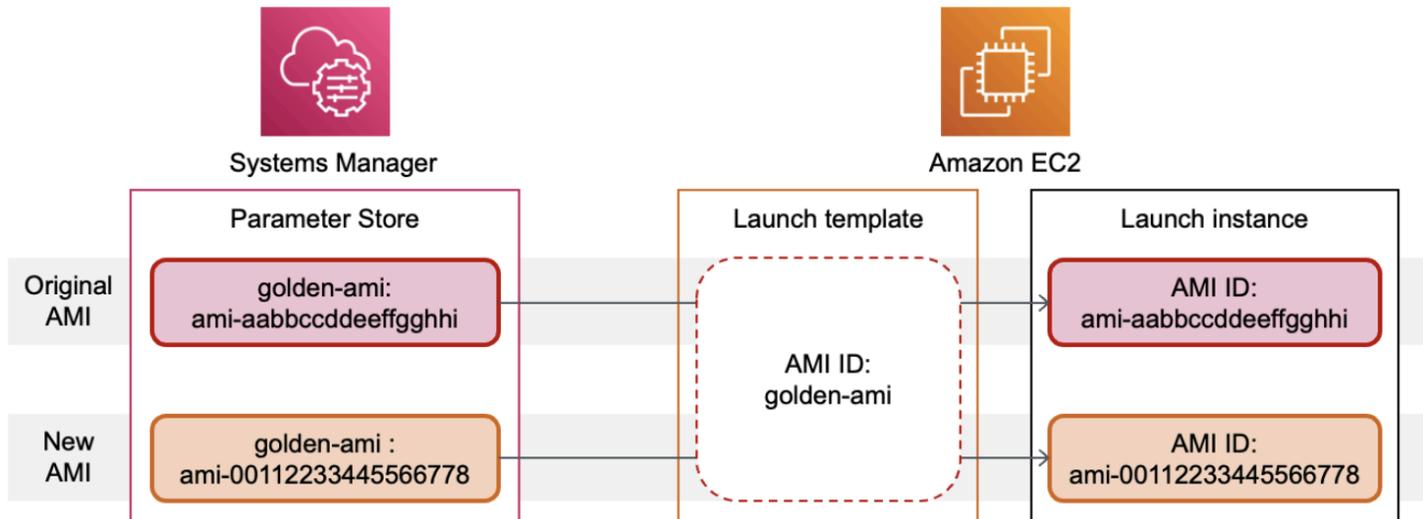
- Utilisez la commande [create-launch-template](#) pour créer un modèle de lancement à l'aide de la sortie de la procédure précédente. Pour plus d'informations sur la création d'un modèle de lancement à l'aide du AWS CLI, consultez [Création d'un modèle de lancement à partir de paramètres](#).

Utilisation d'un paramètre Systems Manager au lieu d'un ID d'AMI

Au lieu de spécifier un ID d'AMI dans vos modèles de lancement, vous pouvez spécifier un paramètre AWS Systems Manager . Si l'ID d'AMI change, vous pouvez le mettre à jour en un seul endroit en mettant à jour le paramètre Systems Manager dans le stockage de paramètres de Systems Manager. Les paramètres peuvent également être partagés avec d'autres Comptes AWS. Vous pouvez stocker et gérer de manière centralisée les paramètres de l'AMI dans un seul compte et les partager avec tous les autres comptes qui ont besoin de les référencer. En utilisant un paramètre Systems Manager, tous vos modèles de lancement peuvent être mis à jour en une seule action.

Un paramètre Systems Manager est une paire clé-valeur définie par l'utilisateur que vous créez dans le stockage de paramètres Systems Manager. Le stockage de paramètres est un endroit central où vous pouvez stocker les valeurs de configuration de votre application. Pour plus d'informations, veuillez consulter la rubrique [AWS Systems Manager Parameter Store](#) dans le Guide de l'utilisateur AWS Systems Manager .

Dans le schéma suivant, le paramètre `golden-ami` est d'abord mappé à l'AMI d'origine `ami-aabbccddeeffgghhi` dans le stockage de paramètres. Dans le modèle de lancement, la valeur de l'ID d'AMI est `golden-ami`. Lorsqu'une instance est lancée à l'aide de ce modèle de lancement, l'ID d'AMI est défini sur `ami-aabbccddeeffgghhi`. Par la suite, l'AMI est mise à jour et un nouvel ID d'AMI est créé. Dans le stockage de paramètres, le paramètre `golden-ami` est mappé au nouveau `ami-00112233445566778`. Le modèle de lancement reste inchangé. Lorsqu'une instance est lancée à l'aide de ce modèle de lancement, l'ID d'AMI devient le nouveau `ami-00112233445566778`.



Format de paramètre Systems Manager pour les ID d'AMI

Les modèles de lancement nécessitent que les paramètres Systems Manager définis par l'utilisateur respectent le format suivant lorsqu'ils sont utilisés à la place d'un ID d'AMI :

- Type de paramètre : `String`
- Type de données de paramètre : `aws:ec2:image` – Cela garantit que le stockage de paramètres vérifie que la valeur que vous entrez est au format approprié pour un ID d'AMI.

Pour plus d'informations sur la création d'un paramètre valide pour un ID d'AMI, consultez [Création de paramètres Systems Manager](#) dans le Guide de l'utilisateur AWS Systems Manager .

Format des paramètres Systems Manager dans les modèles de lancement

Pour utiliser un paramètre Systems Manager à la place d'un ID d'AMI dans un modèle de lancement, vous devez utiliser l'un des formats suivants lorsque vous spécifiez le paramètre dans le modèle de lancement :

Pour référencer un paramètre public :

- `resolve:ssm:public-parameter`

Pour référencer un paramètre stocké dans le même compte :

- `resolve:ssm:parameter-name`
- `resolve:ssm:parameter-name:version-number` – Le numéro de version lui-même est une étiquette par défaut
- `resolve:ssm:parameter-name:label`

Pour référencer un paramètre partagé par un autre Compte AWS :

- `resolve:ssm:parameter-ARN`
- `resolve:ssm:parameter-ARN:version-number`
- `resolve:ssm:parameter-ARN:label`

Versions des paramètres

Les paramètres Systems Manager sont des ressources versionnées. Lorsque vous mettez à jour un paramètre, vous créez de nouvelles versions successives du paramètre. Systems Manager prend en charge les [étiquettes de paramètres](#) que vous pouvez associer à des versions spécifiques d'un paramètre.

Par exemple, le paramètre `golden-ami` peut avoir trois versions : 1, 2 et 3. Vous pouvez créer une étiquette de paramètre `beta` qui correspond à la version 2 et une étiquette de paramètre `prod` qui correspond à la version 3.

Dans un modèle de lancement, vous pouvez spécifier la version 3 du paramètre `golden-ami` en utilisant l'un des formats suivants :

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

La spécification de la version ou de l'étiquette est facultative. Si aucune version ou étiquette n'est spécifiée, c'est la dernière version du paramètre qui est utilisée.

Spécifier un paramètre Systems Manager dans un modèle de lancement

Vous pouvez spécifier un paramètre Systems Manager dans un modèle de lancement au lieu d'un ID d'AMI lorsque vous créez un modèle de lancement ou une nouvelle version d'un modèle de lancement.

Console

Pour spécifier un paramètre Systems Manager dans un modèle de lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement, puis Créer un modèle de lancement.
3. Pour Nom du modèle de lancement, entrez un nom descriptif pour le modèle.
4. Sous Application and OS Images (Amazon Machine Image) (Images d'applications et de systèmes d'exploitation (Amazon Machine Image)), choisissez Browse more AMIs (Parcourir plus d'AMI).
5. Sélectionnez le bouton fléché à droite de la barre de recherche, puis choisissez Spécifier une valeur personnalisée/un paramètre Systems Manager.
6. Dans la boîte de dialogue Spécifier une valeur personnalisée ou un paramètre Systems Manager, procédez comme suit :
 - a. Pour ID d'AMI ou chaîne de paramètres Systems Manager, saisissez le nom du paramètre Systems Manager en utilisant l'un des formats suivants :

Pour référencer un paramètre public :

- **resolve:ssm:*public-parameter***

Pour référencer un paramètre stocké dans le même compte :

- **resolve:ssm:*parameter-name***
- **resolve:ssm:*parameter-name:version-number***
- **resolve:ssm:*parameter-name:label***

Pour référencer un paramètre partagé par un autre Compte AWS :

- **resolve:ssm:*parameter-ARN***
- **resolve:ssm:*parameter-ARN:version-number***
- **resolve:ssm:*parameter-ARN:Label***

b. Choisissez Enregistrer.

7. Spécifiez tout autre paramètre de modèle de lancement selon vos besoins, puis choisissez Créer un modèle de lancement.

Pour plus d'informations, consultez [Création d'un modèle de lancement à partir de paramètres](#).

AWS CLI

Pour spécifier un paramètre Systems Manager dans un modèle de lancement

- Utilisez la commande [create-launch-template](#) pour créer le modèle de lancement. Pour spécifier l'AMI à utiliser, saisissez le nom du paramètre Systems Manager en utilisant l'un des formats suivants :

Pour référencer un paramètre public :

- **resolve:ssm:*public-parameter***

Pour référencer un paramètre stocké dans le même compte :

- **resolve:ssm:*parameter-name***
- **resolve:ssm:*parameter-name:version-number***
- **resolve:ssm:*parameter-name:Label***

Pour référencer un paramètre partagé par un autre Compte AWS :

- **resolve:ssm:*parameter-ARN***
- **resolve:ssm:*parameter-ARN:version-number***
- **resolve:ssm:*parameter-ARN:Label***

L'exemple suivant crée un modèle de lancement qui spécifie ce qui suit :

- Nom du modèle de lancement (*TemplateForWebServer*)

- Une balise pour le modèle de lancement (*purpose=production*)
- Les données de la configuration de l'instance, spécifiées dans un fichier JSON :
 - L'AMI à utiliser (*resolve:ssm:golden-ami*)
 - Le type d'instance à lancer (*m5.4xlarge*)
 - Une balise pour l'instance (*Name=webserver*)

```
aws ec2 create-launch-template \  
  --launch-template-name TemplateForWebServer \  
  --tag-specifications 'ResourceType=launch-  
template,Tags=[{Key=purpose,Value=production}]' \  
  --launch-template-data file://template-data.json
```

Voici un exemple de fichier JSON contenant les données du modèle de lancement pour la configuration de l'instance. La valeur pour ImageId est le nom du paramètre Systems Manager, saisi au format requis *resolve:ssm:golden-ami*.

```
{"LaunchTemplateData": {  
  "ImageId": "resolve:ssm:golden-ami",  
  "InstanceType": "m5.4xlarge",  
  "TagSpecifications": [{  
    "ResourceType": "instance",  
    "Tags": [{  
      "Key": "Name",  
      "Value": "webserver"  
    }]  
  }]  
}
```

Vérifiez qu'un modèle de lancement obtient le bon ID d'AMI

Pour convertir le paramètre Systems Manager en ID AMI réel

Utilisez la commande [describe-launch-template-versions](#) et incluez le paramètre. `--resolve-alias`

```
aws ec2 describe-launch-template-versions \  
  --launch-template-name my-launch-template \  
  --versions $Default \  
  --resolve-alias
```

```
--resolve-alias
```

La réponse inclut l'ID d'AMI pour `ImageId`. Dans cet exemple, lorsqu'une instance est lancée à l'aide de ce modèle de lancement, l'ID de l'AMI est converti en `ami-0ac394d6a3example`.

```
{
  "LaunchTemplateVersions": [
    {
      "LaunchTemplateId": "lt-089c023a30example",
      "LaunchTemplateName": "my-launch-template",
      "VersionNumber": 1,
      "CreateTime": "2022-12-28T19:52:27.000Z",
      "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
      "DefaultVersion": true,
      "LaunchTemplateData": {
        "ImageId": "ami-0ac394d6a3example",
        "InstanceType": "t3.micro",
      }
    }
  ]
}
```

Ressources connexes

Pour plus d'informations sur l'utilisation des paramètres de Systems Manager, consultez les documents de référence suivants dans la documentation de Systems Manager.

- Pour plus d'informations sur la façon de rechercher les paramètres publics de l'AMI pris en charge par Amazon EC2, consultez la section Appeler les paramètres [publics de l'AMI](#).
- Pour plus d'informations sur le partage de paramètres avec d'autres AWS comptes ou via d'autres comptes AWS Organizations, consultez la section [Utilisation de paramètres partagés](#).
- Pour plus d'informations sur le suivi de la création réussie de vos paramètres, consultez la section [Prise en charge des paramètres natifs pour les Amazon Machine Image ID](#).

Limites

- Actuellement, les flottes EC2 et les parcs d'instances Spot ne prennent pas en charge l'utilisation d'un modèle de lancement pour lequel un paramètre Systems Manager est spécifié à la place d'un ID d'AMI. Pour les flottes EC2 et les parcs d'instances Spot, si vous spécifiez une AMI dans le modèle de lancement, vous devez spécifier l'ID d'AMI.

- Amazon EC2 Auto Scaling propose d'autres restrictions. Pour plus d'informations, consultez la section [Utiliser des AWS Systems Manager paramètres plutôt que des ID d'AMI dans les modèles de lancement](#) du manuel Amazon EC2 Auto Scaling User Guide.

Modifier un modèle de lancement (gérer les versions du modèle de lancement)

Les modèles de lancement sont inaltérables ; une fois que vous avez créé un modèle de lancement, vous ne pouvez plus le modifier. Au lieu de cela, vous pouvez créer une nouvelle version du modèle de lancement qui inclut toutes les modifications nécessaires.

Vous pouvez créer différentes versions d'un modèle de lancement, définir la version par défaut, décrire une version de modèle de lancement et supprimer les versions dont vous n'avez plus besoin.

Tâches

- [Créer une version d'un modèle de lancement](#)
- [Définir la version par défaut du modèle de lancement](#)
- [Décrire une version du modèle de lancement](#)
- [Supprimer une version d'un modèle de lancement](#)

Créer une version d'un modèle de lancement

Lorsque vous créez une version d'un modèle de lancement, vous pouvez spécifier de nouveaux paramètres de lancement ou utiliser une version existante comme base de la nouvelle version. Pour plus d'informations sur les paramètres de lancement, consultez [Création d'un modèle de lancement](#).

Console

Pour créer une version d'un modèle de lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Sélectionnez un modèle de lancement, puis choisissez Actions, Modify template (Create new version) (Modifier le modèle (Créer une nouvelle version)).
4. Pour Description de la version du modèle, saisissez une description pour cette version du modèle de lancement.

5. (Facultatif) Développez Modèle source et sélectionnez une version du modèle de lancement à utiliser comme base pour la nouvelle version du modèle. La nouvelle version de modèle de lancement hérite des paramètres de lancement de cette version.
6. Modifiez les paramètres de lancement si nécessaire, puis choisissez Créer un modèle de lancement.

AWS CLI

Pour créer une version d'un modèle de lancement

- Utilisez la commande [create-launch-template-version](#). Vous pouvez spécifier une version source sur laquelle baser la nouvelle version. La nouvelle version hérite des paramètres de lancement de cette version et vous pouvez les remplacer en utilisant `--launch-template-data`. L'exemple suivant illustre la création d'une nouvelle version basée sur la version 1 du modèle de lancement et la spécification d'un autre ID d'AMI.

```
aws ec2 create-launch-template-version \  
  --launch-template-id lt-0abcd290751193123 \  
  --version-description WebVersion2 \  
  --source-version 1 \  
  --launch-template-data "ImageId=ami-c998b6b2"
```

Définir la version par défaut du modèle de lancement

Vous pouvez définir la version par défaut du modèle de lancement. Si vous lancez une instance à partir d'un modèle de lancement sans spécifier de version, le lancement est effectué à l'aide des paramètres de la version par défaut.

Console

Pour définir la version par défaut du modèle de lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Sélectionnez le modèle de lancement et choisissez Actions, Définir la version par défaut.
4. Pour Version du modèle, sélectionnez le numéro de la version à définir par défaut et choisissez Définir comme version par défaut.

AWS CLI

Pour définir la version par défaut du modèle de lancement

- Utilisez la commande [modify-launch-template](#) et spécifiez la version que vous souhaitez définir comme version par défaut.

```
aws ec2 modify-launch-template \  
  --launch-template-id lt-0abcd290751193123 \  
  --default-version 2
```

Décrire une version du modèle de lancement

À l'aide de la console, vous pouvez afficher toutes les versions du modèle de lancement sélectionné ou obtenir une liste des modèles de lancement dont la version la plus récente ou par défaut correspond à un numéro de version spécifique. À l'aide du AWS CLI, vous pouvez décrire toutes les versions, les versions individuelles ou une série de versions d'un modèle de lancement spécifique. Vous pouvez également décrire toutes les dernières versions ou toutes les versions par défaut de tous les modèles de lancement de votre compte.

Console

Pour décrire une version du modèle de lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Vous pouvez afficher une version d'un modèle de lancement spécifique ou obtenir une liste des modèles de lancement dont la version la plus récente ou par défaut correspond à un numéro de version spécifique.
 - Pour afficher une version d'un modèle de lancement : sélectionnez le modèle de lancement. Sous l'onglet Versions dans Version, sélectionnez une version pour afficher ses détails.
 - Pour obtenir une liste de tous les modèles de lancement dont la dernière version correspond à un numéro de version spécifique : dans la barre de recherche, choisissez Dernière version, puis sélectionnez un numéro de version.

- Pour obtenir la liste de tous les modèles de lancement dont la version par défaut correspond à un numéro de version spécifique : dans la barre de recherche, choisissez Version par défaut, puis sélectionnez un numéro de version.

AWS CLI

Pour décrire une version du modèle de lancement

- Utilisez la commande [describe-launch-template-versions](#) et spécifiez les numéros de version. Dans l'exemple suivant, les versions **1** et **3** sont spécifiées.

```
aws ec2 describe-launch-template-versions \  
  --launch-template-id lt-0abcd290751193123 \  
  --versions 1 3
```

Pour décrire toutes les versions du modèle de lancement les plus récentes et par défaut de votre compte

- Utilisez la commande [describe-launch-template-versions](#) et spécifiez `$Latest`, `$Default` ou les deux. Vous devez omettre l'ID et le nom du modèle de lancement dans l'appel. Vous ne pouvez pas spécifier de numéros de version.

```
aws ec2 describe-launch-template-versions \  
  --versions "$Latest,$Default"
```

Supprimer une version d'un modèle de lancement

Si vous n'avez plus besoin d'une version du modèle de lancement, vous pouvez la supprimer.

Considérations

- Vous ne pouvez pas remplacer le numéro d'une version après l'avoir supprimée.
- Vous ne pouvez pas supprimer la version par défaut du modèle de lancement et devez d'abord attribuer une autre version comme version par défaut. Si la version par défaut est la seule version du modèle de lancement, vous devez [supprimer la totalité du modèle de lancement](#).
- Lorsque vous utilisez la console, vous pouvez supprimer une version du modèle de lancement à la fois. Lorsque vous utilisez le AWS CLI, vous pouvez supprimer jusqu'à 200 versions de modèles de

lancement en une seule demande. Pour supprimer plus de 200 versions en une seule demande, vous pouvez [supprimer le modèle de lancement](#), ce qui supprime également toutes ses versions.

Console

Pour supprimer une version du modèle de lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Sélectionnez le modèle de lancement et choisissez Actions, Supprimer la version du modèle.
4. Sélectionnez la version à supprimer et choisissez Supprimer.

AWS CLI

Pour supprimer une version du modèle de lancement

- Utilisez la commande [delete-launch-template-versions](#) et spécifiez les numéros de version à supprimer. Vous pouvez spécifier jusqu'à 200 versions de modèles de lancement à supprimer en une seule demande.

```
aws ec2 delete-launch-template-versions \  
  --launch-template-id lt-0abcd290751193123 \  
  --versions 1
```

Supprimer un modèle de lancement

Si vous n'avez plus besoin d'un modèle de lancement, vous pouvez le supprimer. La suppression d'un modèle de lancement entraîne celle de toutes ses versions. Pour supprimer une version spécifique du modèle de lancement, veuillez consulter [Supprimer une version d'un modèle de lancement](#).

Lorsque vous supprimez un modèle de lancement, cela n'a aucune incidence sur les instances que vous avez lancées à partir de ce modèle de lancement.

Console

Suppression d'un modèle de lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Sélectionnez le modèle de lancement et choisissez Actions, Supprimer le modèle.
4. Entrez **Delete** pour confirmer la suppression, puis choisissez Supprimer.

AWS CLI

Pour supprimer un modèle de lancement

- Utilisez la commande [delete-launch-template](#) (AWS CLI) et spécifiez le modèle de lancement.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

Lancer des instances à partir d'un modèle de lancement

Les modèles de lancement sont pris en charge par plusieurs services de lancement d'instance. Cette rubrique explique comment utiliser un modèle de lancement lors du lancement d'une instance à l'aide de l'assistant de lancement d'instance EC2, d'Amazon EC2 Auto Scaling, de la flotte EC2 et du parc d'instances Spot.

Rubriques

- [Lancer une instance à partir d'un modèle de lancement](#)
- [Utiliser des modèles de lancement avec Amazon EC2 Auto Scaling](#)
- [Utiliser des modèles de lancement avec flotte EC2](#)
- [Utiliser des modèles de lancement avec les parc d'instances Spot](#)

Lancer une instance à partir d'un modèle de lancement

Vous pouvez utiliser les paramètres contenus dans un modèle de lancement pour lancer une instance. Avant de lancer l'instance, vous pouvez remplacer ou ajouter des paramètres de lancement.

Deux balises accompagnées des clés `aws:ec2launchtemplate:id` et `aws:ec2launchtemplate:version` sont attribuées automatiquement aux instances lancées à l'aide d'un modèle de lancement. Vous ne pouvez ni supprimer ni modifier ces balises.

Console

Pour lancer une instance à partir d'un modèle de lancement à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement.
3. Sélectionnez le modèle de lancement et choisissez Actions, Lancement d'une instance à partir d'un modèle.
4. Pour Version du modèle source, sélectionnez la version du modèle de lancement à utiliser.
5. Pour Nombre d'instances, spécifiez le nombre d'instances à lancer.
6. (Facultatif) Vous pouvez remplacer ou ajouter des paramètres du modèle de lancement dans la section Détails de l'instance.
7. Choisissez Lancer une instance à partir d'un modèle.

AWS CLI

Pour lancer une instance à partir d'un modèle de lancement à l'aide de l' AWS CLI

- Utilisez la commande [run-instances](#) et spécifiez le paramètre `--launch-template`. Spécifiez éventuellement la version du modèle de lancement à utiliser. Si vous ne la spécifiez pas, c'est la version par défaut qui est utilisée.

```
aws ec2 run-instances \  
  --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Pour remplacer un paramètre du modèle de lancement, spécifiez-le dans la commande [run-instances](#). Dans l'exemple suivant, le type d'instance spécifié dans le modèle de lancement (le cas échéant) est remplacé.

```
aws ec2 run-instances \  
  --launch-template LaunchTemplateId=lt-0abcd290751193123 \  
  --instance-type t2.small
```

- Si vous spécifiez un paramètre imbriqué faisant partie d'une structure complexe, l'instance est lancée à l'aide de la structure complexe spécifiée dans le modèle de lancement et des éventuels paramètres imbriqués supplémentaires définis.

Dans l'exemple suivant, l'instance est lancée avec la balise `Owner=TeamA` et toute autre balise spécifiée dans le modèle de lancement. Si le modèle de lancement comporte une balise avec une clé `Owner`, la valeur est remplacée par `TeamA`.

```
aws ec2 run-instances \  
  --launch-template LaunchTemplateId=lt-0abcd290751193123 \  
  --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

Dans l'exemple suivant, l'instance est lancée avec un volume pourvu du nom de périphérique `/dev/xvdb` et d'autres mappages de périphérique de stockage en mode bloc spécifiés dans le modèle de lancement. Si le modèle de lancement possède un volume existant défini pour `/dev/xvdb`, ses valeurs sont remplacées par celles qui sont spécifiées.

```
aws ec2 run-instances \  
  --launch-template LaunchTemplateId=lt-0abcd290751193123 \  
  --block-device-mappings "DeviceName=/dev/  
xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez [Résoudre les problèmes de lancement d'instance](#).

PowerShell

Pour lancer une instance à partir d'un modèle de lancement à l'aide de l'AWS Tools for PowerShell

- Utilisez la [New-EC2Instance](#) commande et spécifiez le `-LaunchTemplate` paramètre. Spécifiez éventuellement la version du modèle de lancement à utiliser. Si vous ne la spécifiez pas, c'est la version par défaut qui est utilisée.

```
Import-Module AWS.Tools.EC2  
New-EC2Instance `  
  -LaunchTemplate (  
    New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -  
Property @{  
  LaunchTemplateId = 'lt-0abcd290751193123';
```

```

        Version      = '4'
    }
)

```

- Pour remplacer un paramètre du modèle de lancement, spécifiez-le dans la [New-EC2Instance](#) commande. Dans l'exemple suivant, le type d'instance spécifié dans le modèle de lancement (le cas échéant) est remplacé.

```

Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
    LaunchTemplateId = 'lt-0abcd290751193123';
    Version          = '4'
}
)

```

- Si vous spécifiez un paramètre imbriqué faisant partie d'une structure complexe, l'instance est lancée à l'aide de la structure complexe spécifiée dans le modèle de lancement et des éventuels paramètres imbriqués supplémentaires définis.

Dans l'exemple suivant, l'instance est lancée avec la balise *Owner=TeamA* et toute autre balise spécifiée dans le modèle de lancement. Si le modèle de lancement comporte une balise avec une clé *Owner*, la valeur est remplacée par *TeamA*.

```

Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
    LaunchTemplateId = 'lt-0abcd290751193123';
    Version          = '4'
}
) `
    -TagSpecification (
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags          = @(
                @{key = "Owner"; value = "TeamA" },

```

```

        @{key = "Department"; value = "Operations" }
    )
}
)

```

Dans l'exemple suivant, l'instance est lancée avec un volume pourvu du nom de périphérique `/dev/xvdb` et d'autres mappages de périphérique de stockage en mode bloc spécifiés dans le modèle de lancement. Si le modèle de lancement possède un volume existant défini pour `/dev/xvdb`, ses valeurs sont remplacées par celles qui sont spécifiées.

```

Import-Module AWS.Tools.EC2
New-EC2Instance `
  -InstanceType t4g.small `
  -LaunchTemplate (
    New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
  LaunchTemplateId = 'lt-0abcd290751193123';
  Version          = '4'
}
) `
  -BlockDeviceMapping (
    New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
      DeviceName = '/dev/xvdb';
      EBS        = (
        New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
          VolumeSize = 25;
          VolumeType = 'gp3'
        }
      )
    }
  )
)

```

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez [Résoudre les problèmes de lancement d'instance](#).

Utiliser des modèles de lancement avec Amazon EC2 Auto Scaling

Vous pouvez créer un groupe Auto Scaling et spécifier un modèle de lancement à utiliser pour le groupe. Lorsque Amazon EC2 Auto Scaling lance des instances dans le groupe Auto Scaling, il utilise les paramètres de lancement définis dans le modèle de lancement associé. Pour plus d'informations,

consultez [Create a launch template for an Auto Scaling group](#) et [Create a launch template using advanced settings in the](#) Amazon EC2 Auto Scaling User Guide.

Avant de pouvoir créer un groupe Auto Scaling à l'aide d'un modèle de lancement, vous devez créer un modèle de lancement qui comprend les paramètres requis pour lancer une instance dans un groupe Auto Scaling, comme l'ID de l'AMI. La console fournit des conseils pour vous aider à créer un modèle que vous pouvez utiliser avec Amazon EC2 Auto Scaling.

Pour créer un modèle de lancement à utiliser avec Auto Scaling à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Modèles de lancement, puis Créer un modèle de lancement.
3. Pour Nom du modèle de lancement, entrez un nom descriptif pour le modèle.
4. Pour Description de la version du modèle, fournissez une brève description de cette version du modèle de lancement.
5. Sous Auto Scaling guidance (Conseils Auto Scaling), cochez la case pour obtenir des conseils d'Amazon EC2 pour créer un modèle à utiliser avec Auto Scaling.
6. Modifiez les paramètres de lancement selon vos besoins. Étant donné que vous avez sélectionné des conseils Auto Scaling, certains champs sont obligatoires et certains ne sont pas disponibles. Pour plus d'informations sur la configuration des paramètres de lancement pour Amazon EC2 Auto Scaling, consultez les sections [Créer un modèle de lancement pour un groupe Auto Scaling](#) et [Créer un modèle de lancement à l'aide des paramètres avancés](#) dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.
7. Choisissez Créer un modèle de lancement.
8. (Facultatif) Pour créer un groupe Auto Scaling à l'aide de ce modèle de lancement, sur la page Next steps (Étapes suivantes), choisissez Create Auto Scaling group (Créer un groupe Auto Scaling).

Pour des exemples illustrant comment utiliser le AWS CLI pour créer des modèles de lancement avec différentes combinaisons de paramètres, consultez la section [Exemples de création et de gestion de modèles de lancement avec le AWS Command Line Interface \(AWS CLI\)](#) dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

Pour créer ou mettre à jour un groupe Auto Scaling avec un modèle de lancement à l'aide du AWS CLI

- Utilisez les commandes [create-auto-scaling-group](#) ou [update-auto-scaling-group](#) et spécifiez le paramètre `--launch-template`.

Pour plus d'informations sur la création ou la mise à jour d'un groupe Auto Scaling à l'aide d'un modèle de lancement, consultez les rubriques suivantes du manuel Amazon EC2 Auto Scaling User Guide.

- [Créez des groupes Auto Scaling à l'aide de modèles de lancement](#)
- [Mettre à jour un groupe Auto Scaling](#)

Utiliser des modèles de lancement avec flotte EC2

Vous pouvez créer une demande flotte EC2 et spécifier un modèle de lancement dans la configuration d'instance. Si Amazon EC2 satisfait à la demande flotte EC2, il utilise les paramètres de lancement définis dans le modèle de lancement associé. Vous pouvez remplacer certains des paramètres spécifiés dans le modèle de lancement.

Pour plus d'informations, consultez [Créer une flotte EC2](#).

Pour créer une flotte EC2 avec un modèle de lancement à l'aide du AWS CLI

- Utilisez la commande [create-fleet](#). Utilisez le paramètre `--launch-template-configs` pour spécifier le modèle de lancement et tous les remplacements de celui-ci.

Utiliser des modèles de lancement avec les parc d'instances Spot

Vous pouvez créer une demande de parc d'instances Spot et spécifier un modèle de lancement dans la configuration de l'instance. Si Amazon EC2 satisfait à la demande de parc d'instances Spot, il utilise les paramètres de lancement définis dans le modèle de lancement associé. Vous pouvez remplacer certains des paramètres spécifiés dans le modèle de lancement.

Pour plus d'informations, consultez [Créer une Spot Fleet request](#).

Pour créer une demande de parc d'instances Spot avec un modèle de lancement à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Choisissez Demander des instances ponctuelles.
4. Sous Launch parameters (Paramètres de lancement), choisissez Use a launch template (Utiliser un modèle de lancement).
5. Pour Launch template (Modèle de lancement), choisissez un modèle de lancement, puis, dans le champ de droite, choisissez la version du modèle de lancement.
6. Configurez votre parc d'instances Spot en sélectionnant différentes options sur cet écran. Pour plus d'informations sur ces options, consultez [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#).
7. Lorsque vous êtes prêt à créer votre parc d'instances Spot, choisissez Launch (Lancer).

Pour créer une demande Spot Fleet avec un modèle de lancement à l'aide du AWS CLI

- Utilisez la commande [request-spot-fleet](#). Utilisez le paramètre `LaunchTemplateConfigs` pour spécifier le modèle de lancement et tous les remplacements de celui-ci.

Lancer une instance à l'aide des paramètres d'une instance existante

La console Amazon EC2 propose une option Launch more like this (Lancer d'autres instances comme celle-ci) qui vous permet d'utiliser une instance actuelle comme base pour lancer d'autres instances. Cette option remplit automatiquement l'assistant de lancement d'instance Amazon EC2 avec certains détails de configuration issus de l'instance sélectionnée.

Considérations

- Nous ne clonons pas vos instances ; nous ne répliquons que certains détails de configuration. Pour créer une copie de l'instance, commencez par créer une AMI sur la base de cette instance, puis lancez des instances supplémentaires à partir de l'AMI. Créez un [modèle de lancement](#) pour vous assurer de lancer vos instances en utilisant les mêmes informations de lancement.
- L'instance doit être dans l'état `running`.

Détails copiés

Les détails de configuration suivants sont copiés de l'instance sélectionnée vers l'assistant de lancement d'instance :

- ID d'AMI
- Type d'instance
- zone de disponibilité ou le VPC et le sous-réseau où se trouve l'instance sélectionnée
- Adresse IPv4 publique. Si l'instance sélectionnée a une adresse IPv4 publique, la nouvelle instance en reçoit une aussi, quel que soit le paramètre d'adresse IPv4 public par défaut de l'instance sélectionnée. Pour plus d'informations sur les adresses IPv4 publiques, consultez [Adresses IPv4 publiques](#).
- Groupe de placement, le cas échéant
- Rôle IAM associé à l'instance, le cas échéant
- Paramètre du comportement lors de la mise hors tension (arrêt ou mise hors service)
- Paramètre de protection de mise hors service de l'instance (vrai ou faux)
- CloudWatch surveillance (activée ou désactivée)
- Paramètre d'optimisation Amazon EBS (vrai ou faux)
- Paramètre de location, en cas de lancement sur un VPC (partagé ou dédié)
- ID du noyau et ID du disque RAM, le cas échéant
- Données utilisateur, le cas échéant
- Balises associées à l'instance, le cas échéant
- Groupes de sécurité associés à l'instance
- [Instances Windows] Informations d'association. Si l'instance sélectionnée est associée à un fichier de configuration, le même fichier est automatiquement associé à la nouvelle instance. Si le fichier de configuration comprend une configuration de domaine joint, la nouvelle instance est jointe au même domaine. Pour plus d'informations sur la jointure d'un domaine, consultez [Seamlessly Join a Windows EC2 Instance](#) (Jonction facile d'une instance Windows EC2) dans le Guide d'administration AWS Directory Service .

Détails non copiés

Les détails de configuration suivants ne sont pas copiés à partir de l'instance sélectionnée. Au lieu de cela, l'assistant applique leurs paramètres ou leur comportement par défaut :

- Nombre d'interfaces réseau : par défaut, il y a une interface réseau, qui est l'interface réseau principale (eth0).
- Stockage : la configuration de stockage par défaut est déterminée par l'AMI et le type d'instance.

Lancement de plus d'instances similaires à une instance existante

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez une instance, puis choisissez Actions, Images et modèles, puis En lancer plus comme ceci.
4. L'assistant de lancement d'instance s'ouvre. Vous pouvez apporter toutes les modifications nécessaires à la configuration de l'instance en sélectionnant différentes options sur cet écran.

Lorsque vous êtes prêt à lancer votre instance, choisissez Launch instance (Lancer l'instance).

5. Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez [Résoudre les problèmes de lancement d'instance](#).

Lancer une AWS Marketplace instance

Vous pouvez vous abonner à un AWS Marketplace produit et lancer une instance depuis l'AMI du produit à l'aide de l'assistant de lancement Amazon EC2. Pour plus d'informations sur les AMI payantes, consultez [AMI payantes](#). Pour annuler votre abonnement après le lancement, vous devez d'abord mettre fin à toutes les instances qui s'exécutent à partir de l'abonnement. Pour plus d'informations, consultez [Gérez vos AWS Marketplace abonnements](#).

New console

Pour lancer une instance à l' AWS Marketplace aide de l'assistant de lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sur le tableau de bord de la console Amazon EC2, sélectionnez Launch instance (Lancer une instance).
3. (Facultatif) Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom descriptif pour votre instance.
4. Sous Application and OS Images (Amazon Machine Image) (Images d'applications et de systèmes d'exploitation), choisissez Browse more AMIs (Parcourir d'autres AMI), puis

choisissez l'onglet AWS Marketplace AMIs (Les AMI). Recherchez une AMI appropriée en parcourant les catégories ou en utilisant la fonctionnalité de recherche. Pour choisir un produit, choisissez Select (Sélectionner).

5. Une fenêtre s'ouvre avec un aperçu du produit que vous avez sélectionné. Vous pouvez afficher les informations de tarification, ainsi que toute autre information communiquée par le fournisseur. Lorsque vous êtes prêt, cliquez sur l'un des boutons suivants :
 - S'abonner au lancement de l'instance : votre abonnement commence lorsque vous choisissez Launch instance (à l'étape 10).
 - Abonnez-vous maintenant — Votre abonnement commence immédiatement. Pendant que l'abonnement est en cours, vous pouvez configurer l'instance en suivant les étapes de cette procédure. En cas de problème avec les informations de votre carte bancaire, vous serez invité à mettre à jour les coordonnées de votre compte.

 Note

Vous n'êtes pas facturé pour l'utilisation du produit tant que vous n'avez pas lancé une instance avec l'AMI. Prenez note de la tarification pour chaque type d'instance pris en charge lorsque vous sélectionnez un type d'instance. Des taxes supplémentaires peuvent également s'appliquer au produit.

6. Pour Instance type (Type d'instance), sélectionnez un type d'instance pour votre instance. Le type d'instance définit la configuration matérielle et la taille de l'instance à lancer.
7. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou créez-en une.
8. Sous Network settings (Paramètres réseau), Firewall (security groups) (Pare-feu (groupes de sécurité)), prenez note du nouveau groupe de sécurité qui a été créé selon les spécifications du fournisseur pour le produit. Le groupe de sécurité peut inclure des règles qui autorisent l'accès à toutes les adresses IPv4 (0.0.0.0/0) sur SSH (port 22) sous Linux ou RDP (port 3389) sous Windows. Il est recommandé d'ajuster ces règles pour n'autoriser qu'une adresse ou plage d'adresses spécifiques à accéder à votre instance sur ces ports.
9. Vous pouvez utiliser les autres champs sur l'écran pour configurer votre instance, ajouter du stockage et ajouter des identifications. Pour plus d'informations sur les différentes options que vous pouvez configurer, consultez [Lancer une instance à l'aide de paramètres définis](#).

10. Dans le panneau Summary (Résumé), sous Software Image (AMI) (Image logicielle), vérifiez les détails de l'AMI à partir de laquelle vous êtes sur le point de lancer l'instance. Vérifiez également les autres détails de configuration que vous avez spécifiés. Lorsque vous êtes prêt à lancer votre instance, choisissez Launch instance (Lancer l'instance).
11. Selon le produit auquel vous êtes abonné, le lancement de l'instance peut prendre quelques minutes, voire plus. Si vous avez choisi S'abonner au lancement de l'instance à l'étape 5, vous êtes d'abord abonné au produit avant que votre instance ne puisse être lancée. En cas de problème avec les informations de votre carte bancaire, vous serez invité à mettre à jour les coordonnées de votre compte. Lorsque la page de confirmation de lancement s'affiche, choisissez View all instances (Afficher toutes les instances) pour accéder à la page Instances.

 Note

Le prix de l'abonnement vous est facturé aussi longtemps que votre instance est dans l'état `running`, même si elle est inactive. Si votre instance est arrêtée, il se peut que vous continuiez à être facturé pour le stockage.

12. Lorsque votre instance est à l'état `running`, vous pouvez vous y connecter. Pour ce faire, sélectionnez votre instance dans la liste, choisissez Connect (Connecter), puis choisissez une option de connexion. Pour plus d'informations sur la connexion à votre instance, consultez [Connectez-vous à votre instance Linux](#) ou [Connexion à votre instance Windows](#).

 Important

Lisez attentivement les instructions d'utilisation du fournisseur, car vous devrez peut-être utiliser un nom d'utilisateur spécifique pour vous connecter à votre instance. Pour plus d'informations sur l'accès aux détails de votre abonnement, consultez [Gérez vos AWS Marketplace abonnements](#).

13. Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez [Résoudre les problèmes de lancement d'instance](#).

Old console

Pour lancer une instance à l'AWS Marketplace aide de l'assistant de lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le tableau de bord Amazon EC2, choisissez Lancer une instance.
3. Sur la page Choose an Amazon Machine Image (AMI), sélectionnez la catégorie AWS Marketplace sur la gauche. Recherchez une AMI appropriée en floutant les catégories ou à l'aide de la fonctionnalité de recherche. Sélectionnez Select pour choisir votre produit.
4. Une présentation du produit sélectionné s'affiche dans une boîte de dialogue. Vous pouvez afficher les informations de tarification, ainsi que toute autre information communiquée par le fournisseur. Lorsque vous êtes prêt, sélectionnez Continue.

 Note

L'utilisation du produit ne vous est plus facturée jusqu'à ce que vous ayez lancé une instance avec l'AMI. Notez la tarification de chaque type d'instance pris en charge, car vous allez être invité à sélectionner un type d'instance sur la page suivante de l'Assistant. Des taxes supplémentaires peuvent également être appliquées au produit.

5. Sur la page Choisir un type d'instance, sélectionnez la configuration matérielle et la taille de l'instance à lancer. Lorsque vous avez terminé, sélectionnez Next: Configure Instance Details.
6. Sur les pages suivantes de l'Assistant, vous pouvez configurer votre instance et ajouter du stockage, ainsi que des balises. Pour plus d'informations sur les différentes options que vous pouvez configurer, consultez [Lancer une instance à l'aide de l'ancien assistant de lancement d'instance](#). Choisissez Next jusqu'à la page Configure Security Group.

L'Assistant crée un groupe de sécurité conforme aux spécifications du fournisseur pour le produit. Le groupe de sécurité peut inclure des règles autorisant l'accès à toutes les adresses IPv4 (0.0.0.0/0) sur SSH (port 22) sur Linux ou sur RDP (port 3389) sur Windows. Il est recommandé d'ajuster ces règles pour n'autoriser qu'une adresse ou plage d'adresses spécifiques à accéder à votre instance sur ces ports.

Lorsque vous êtes prêt, sélectionnez Review and Launch.

7. Sur la page Review Instance Launch, vérifiez les détails de l'AMI à partir de laquelle vous vous apprêtez à lancer l'instance, ainsi que les autres détails de configuration que vous avez définis dans l'Assistant. Lorsque vous êtes prêt, sélectionnez Launch pour choisir ou créer une paire de clés, et démarrez votre instance.
8. Selon le produit auquel vous êtes abonné, le lancement de l'instance peut prendre quelques minutes, voire plus. Vous devez vous abonner au produit avant de pouvoir lancer une

instance. En cas de problème avec les informations de votre carte bancaire, vous serez invité à mettre à jour les coordonnées de votre compte. Lorsque la page de confirmation de lancement s'affiche, sélectionnez View Instances pour accéder à la page Instances.

 Note

Vous êtes facturé pour le prix de l'abonnement aussi longtemps que votre instance s'exécute, même si elle est inactive. Si votre instance est arrêtée, il se peut que vous continuiez à être facturé pour le stockage.

9. Lorsque votre instance est à l'état `running`, vous pouvez vous y connecter. Pour ce faire, sélectionnez votre instance dans la liste et choisissez Connect. Suivez les instructions de la boîte de dialogue. Pour plus d'informations sur la connexion à votre instance, consultez [Connectez-vous à votre instance Linux](#) ou [Connexion à votre instance Windows](#).

 Important

Lisez attentivement les instructions d'utilisation du fournisseur, car il se peut que vous deviez choisir un nom utilisateur spécifique pour vous connecter à l'instance. Pour plus d'informations sur l'accès aux détails de votre abonnement, consultez [Gérez vos AWS Marketplace abonnements](#).

10. Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez [Résoudre les problèmes de lancement d'instance](#).

Lancer une instance AWS Marketplace AMI à l'aide de l'API et de la CLI

Pour lancer des instances à partir de AWS Marketplace produits à l'aide de l'API ou des outils de ligne de commande, assurez-vous d'abord que vous êtes abonné au produit. Vous pouvez alors lancer une instance avec l'ID d'AMI du produit en utilisant les méthodes suivantes :

Méthode	Documentation
AWS CLI	Utilisez la commande run-instances ou consultez la rubrique suivante pour plus d'informations : Lancement d'une instance .

Méthode	Documentation
AWS Tools for Windows PowerShell	Utilisez la New-EC2Instance commande ou consultez la rubrique suivante pour plus d'informations : Lancer une instance Amazon EC2 à l'aide de Windows PowerShell
API de requête	Utilisez la RunInstances demande.

Arrêtez et démarrez les instances Amazon EC2

Vous pouvez arrêter et démarrer votre instance si elle comporte un volume Amazon EBS comme périphérique racine. Lorsque vous arrêtez une instance, elle s'arrête. Lorsque vous démarrez une instance, celle-ci est généralement migrée vers un nouvel ordinateur hôte sous-jacent et une nouvelle adresse IPv4 publique lui est attribuée.

Lorsque vous arrêtez une instance, elle n'est pas supprimée. Si vous jugez que vous n'avez plus besoin d'une instance, vous pouvez y mettre fin. Pour plus d'informations, consultez [Mettre fin aux instances Amazon EC2](#). Si vous souhaitez mettre une instance en veille prolongée pour enregistrer le contenu de la mémoire de l'instance (RAM), consultez [Hibernez votre instance Amazon EC2](#). Pour connaître les différences entre les actions du cycle de vie des instances, consultez [Différences entre redémarrage, arrêt, mise en veille prolongée et résiliation](#).

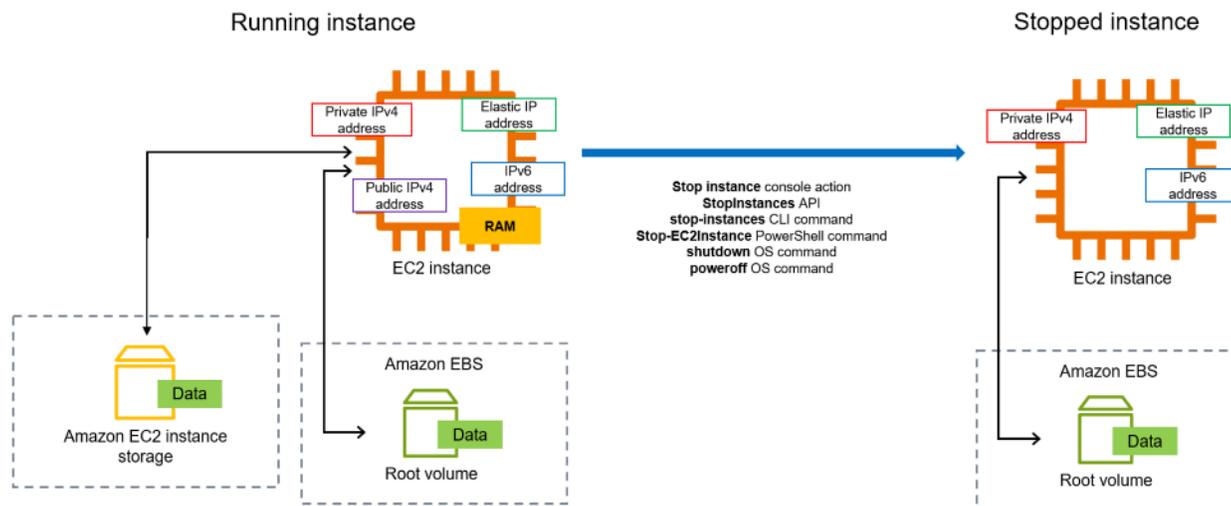
Table des matières

- [Fonctionnement de l'arrêt et du démarrage d'une instance](#)
- [Arrêtez et démarrez manuellement vos instances](#)
- [Arrêter et démarrer automatiquement vos instances](#)
- [Trouver toutes les instances en cours d'exécution et arrêtées](#)
- [Activez la protection anti-arrêt pour votre instance](#)

Fonctionnement de l'arrêt et du démarrage d'une instance

Lorsque vous arrêtez une instance, les modifications sont enregistrées au niveau du système d'exploitation de l'instance, certaines ressources sont perdues et certaines ressources persistent. Lorsque vous démarrez une instance, les modifications sont enregistrées au niveau de l'instance.

Le schéma suivant montre ce qui est perdu et ce qui persiste lorsqu'une instance Amazon EC2 est arrêtée. Lorsqu'une instance s'arrête, elle perd tous les volumes de stockage d'instances attachés et les données stockées sur ces volumes, les données stockées sur la RAM de l'instance et l'adresse IPv4 publique attribuée si aucune adresse IP Elastic n'est associée à l'instance. Une instance conserve les adresses IPv4 privées qui lui sont attribuées, les adresses IP Elastic associées à l'instance, toutes les adresses IPv6 et tous les volumes Amazon EBS attachés ainsi que les données de ces volumes.



Ce qui se passe lorsque vous arrêtez une instance

Modifications enregistrées au niveau du système d'exploitation

- La demande d'API envoie un événement d'appui sur un bouton à l'invité.
- Divers services système sont arrêtés à la suite de l'événement d'appui sur le bouton. L'arrêt normal est déclenché par l'événement d'appui sur un bouton d'arrêt ACPI à partir de l'hyperviseur.
- L'arrêt ACPI est lancé.
- L'instance s'arrête lorsque le processus d'arrêt normal se termine. L'heure d'arrêt du système d'exploitation n'est pas configurable.
- Si le système d'exploitation d'instance ne s'arrête pas proprement en quelques minutes, un arrêt dur est effectué.
- L'instance cesse de s'exécuter.
- L'état de l'instance devient `stopping`, puis `stopped`.
- [Auto Scaling] Si votre instance est un groupe Auto Scaling, lorsque l'instance se trouve dans un état Amazon EC2 autre que `running`, ou si son état pour les vérifications d'état passe à

impaired, Amazon EC2 Auto Scaling considère que l'instance est défectueuse et la remplace. Pour plus d'informations, consultez [Vérifications de l'état pour les instances Auto Scaling](#) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

- [Instances Windows] Lorsque vous arrêtez et démarrez une instance Windows, l'agent de lancement exécute des tâches sur l'instance, telles que la modification des lettres du lecteur pour tous les volumes Amazon EBS attachés. Pour plus d'informations sur ces valeurs par défaut et sur la manière dont vous pouvez les modifier, consultez [the section called "EC2Launch v2"](#).

Ressources perdues

- Les données stockées dans la RAM.
- Les données stockées sur les volumes de stockage d'instances.
- L'adresse IPv4 publique qu'Amazon EC2 a automatiquement attribuée à l'instance au lancement ou au démarrage. Pour retenir une adresse IPv4 publique qui ne change jamais, vous pouvez associer une [adresse IP Elastic](#) à votre instance.

Des ressources qui persistent

- Tous les volumes Amazon EBS attachés.
- Les données stockées dans les volumes Amazon EBS attachés.
- Les adresses IPv4 privées.
- Les adresses IPv6.
- Les adresses IP élastiques associées à l'instance. Veuillez noter que lorsque l'instance est arrêtée, nous [commençons à vous facturer les adresses IP Elastic associées](#).

Pour plus d'informations sur ce qui se passe lorsque vous arrêtez une instance Mac, consultez [the section called "Arrêt ou résiliation de votre instance Mac"](#).

Ce qui se passe lorsque vous lancer une instance

Modifications enregistrées au niveau du système d'exploitation

- L'instance est généralement migrée vers un nouvel ordinateur hôte sous-jacent (même si, dans certains cas, comme lorsqu'une instance est allouée à un hôte dans une configuration [Hôte dédié](#), elle reste sur l'hôte actuel).

- Amazon EC2 attribue une nouvelle adresse IPv4 publique à l'instance si l'instance est configurée pour recevoir une adresse IPv4 publique. Pour retenir une adresse IPv4 publique qui ne change jamais, vous pouvez associer une [adresse IP Elastic](#) à votre instance.

Tester la réponse de l'application pour l'arrêt et le démarrage

Vous pouvez utiliser AWS Fault Injection Service pour tester la façon dont votre application répond lorsque votre instance est arrêtée et démarrée. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Fault Injection Service](#).

Coûts liés à l'arrêt et au démarrage de l'instance

Les coûts suivants sont associés à l'arrêt et au démarrage d'une instance.

Arrêt : dès que l'état d'une instance passe à `shutting-down` ou `terminated`, l'instance ne vous est plus facturée. Aucuns frais d'utilisation ou de transfert de données ne vous sont facturés pour une instance arrêtée. Des frais sont facturés pour stocker les volumes de stockage Amazon EBS.

Démarrage : chaque fois que vous démarrez une instance arrêtée, nous facturons au minimum une minute d'utilisation. Après une minute, seules les secondes que vous utilisez vous sont facturées. Si, par exemple, vous exécutez une instance pendant 20 secondes, puis que vous l'arrêtez, nous vous facturons une minute complète. Si vous exécutez une instance pendant 3 minutes et 40 secondes, nous vous facturons exactement 3 minutes et 40 secondes d'utilisation.

Arrêtez et démarrez manuellement vos instances

Vous pouvez arrêter et démarrer vos instances basées sur Amazon EBS (instances dotées d'appareils racines EBS). Vous ne pouvez pas arrêter et démarrer des instances avec le périphérique racine du stockage d'instance.

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Avant d'arrêter une instance, vérifiez que vous avez copié toutes les données dont vous avez besoin depuis les volumes de stockage de l'instance vers un stockage persistant, tel qu'Amazon EBS ou Amazon S3.

Console

Pour arrêter et démarrer une instance basée sur Amazon EBS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation de gauche, choisissez Instances, puis sélectionnez l'instance.
3. Dans l'onglet Stockage, vérifiez que le type de périphérique racine est EBS. Dans le cas contraire, vous ne pouvez pas arrêter l'instance.
4. Choisissez État de l'instance, Arrêter l'instance. Si cette option est désactivée, l'instance est déjà arrêtée ou son périphérique racine est un volume de stockage d'instances.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter. L'arrêt de l'instance peut prendre quelques minutes.
6. Pour démarrer une instance arrêtée, sélectionnez l'instance et choisissez État de l'instance, Démarrer l'instance.
7. Il peut s'écouler quelques minutes avant que l'instance ne passe à l'état `running`.
8. Si vous avez arrêté une instance basée sur Amazon EBS et que celle-ci semble « bloquée » à l'état `stopping`, vous pouvez forcer son arrêt. Pour plus d'informations, consultez [Résoudre les problèmes d'arrêt de votre instance](#).

Command line

Prérequis

Vérifiez que le périphérique racine de l'instance est un volume EBS. Par exemple, exécutez la AWS CLI commande [describe-instances](#) et vérifiez que ce `RootDeviceType` n'est pas le cas. `instance-store`

Pour arrêter et démarrer une instance basée sur Amazon EBS

Utilisez l'une des commandes suivantes :

- AWS CLI : [stop-instances](#) et [start-instances](#).
- AWS Tools for PowerShell— [Stop-EC2Instance](#) et [Start-EC2Instance](#).
- Commandes du système d'exploitation : vous pouvez lancer un arrêt à l'aide des commandes `shutdown` ou `poweroff`. Lorsque vous utilisez une commande du système d'exploitation, l'instance s'arrête par défaut. Vous pouvez modifier ce comportement pour que l'instance

prene fin. Pour plus d'informations, consultez [Modifier le comportement d'arrêt lancé de l'instance](#).

[Instances Linux] L'utilisation de la halt commande du système d'exploitation depuis une instance ne déclenche pas d'arrêt. Si vous utilisez la commande halt, l'instance n'est pas résiliée. Au lieu de cela, elle place le CPU à l'état HLT, ce qui suspend le fonctionnement du CPU. L'instance reste en cours d'exécution.

Arrêter et démarrer automatiquement vos instances

Vous pouvez automatiser l'arrêt et le démarrage de vos instances à l'aide des services suivants :

Planificateur d'instance activé AWS

Vous pouvez utiliser le planificateur d'instance activé AWS pour automatiser le démarrage et l'arrêt des instances EC2. Pour plus d'informations, consultez [Comment utiliser le planificateur d'instance CloudFormation pour planifier des instances EC2 ?](#) Notez que [des frais supplémentaires sont facturés](#).

AWS Lambda et une EventBridge règle Amazon

Vous pouvez utiliser Lambda et une EventBridge règle pour arrêter et démarrer vos instances selon un calendrier. Pour plus d'informations, consultez [Comment utiliser Lambda pour arrêter et démarrer des instances Amazon EC2 à intervalles réguliers ?](#)

Amazon EC2 Auto Scaling

Pour vous assurer que vous disposez du bon nombre d'instances Amazon EC2 disponibles pour gérer la charge d'une application, créez des groupes Auto Scaling. Amazon EC2 Auto Scaling garantit que votre application dispose toujours de la bonne capacité pour gérer la demande de trafic et permet de réduire les coûts en lançant des instances uniquement lorsqu'elles sont nécessaires. Veuillez noter que Amazon EC2 Auto Scaling résilie les instances inutiles plutôt que de les arrêter. Pour configurer des groupes Auto Scaling, consultez [Commencer avec Amazon EC2 Auto Scaling](#) (français non garanti).

Trouver toutes les instances en cours d'exécution et arrêtées

Vous pouvez trouver toutes vos instances en cours d'exécution et arrêtées Régions AWS sur une seule page à l'aide d'[Amazon EC2 Global View](#). Cette capacité est particulièrement utile pour faire

l'inventaire et rechercher les instances oubliées. Pour plus d'informations sur l'utilisation de Global View, consultez [Amazon EC2 Global View \(Amazon EC2 Global View\)](#).

Activez la protection anti-arrêt pour votre instance

Pour éviter qu'une instance ne soit arrêtée accidentellement, vous pouvez activer la protection contre l'arrêt de l'instance. La protection contre l'arrêt protège également votre instance contre la résiliation accidentelle.

L'attribut `DisableApiStop` de l'[ModifyInstanceAttribute](#) API Amazon EC2 détermine si l'instance peut être arrêtée à l'aide de la console Amazon EC2, de l'API Amazon EC2 ou de AWS CLI l'API Amazon EC2. Vous pouvez définir la valeur de cet attribut lorsque vous lancez l'instance, pendant l'exécution de l'instance ou une fois l'instance arrêtée.

Considérations

- L'activation de la protection contre les arrêts ne vous empêche pas d'arrêter accidentellement une instance en déclenchant un arrêt à partir de l'instance à l'aide d'une commande du système d'exploitation telle que shutdown ou poweroff.
- L'activation de la protection d'arrêt n'empêche pas l'arrêt de l'instance lorsqu'un [événement planifié](#) est prévu pour arrêter l'instance.
- L'activation de la protection contre l'arrêt n'empêche pas Amazon EC2 Auto Scaling de résilier une instance lorsque celle-ci n'est pas saine ou pendant des événements de mise à l'échelle horizontale. Vous pouvez contrôler si un groupe Auto Scaling peut résilier une instance en particulier lors de la diminution de la taille en utilisant la [protection contre la diminution de la taille d'instance](#).
- La protection anti-arrêt empêche non seulement l'arrêt accidentel de votre instance, mais également son arrêt accidentel lors de l'utilisation de la console ou de l'API. AWS CLI Cependant, cela ne définit pas automatiquement l'attribut `DisableApiTermination`. Notez que lorsque l'attribut `DisableApiStop` est défini sur `false`, le paramètre `DisableApiTermination` d'attribut détermine si l'instance peut être interrompue à l'aide de la console ou de l'API. AWS CLI Pour plus d'informations, consultez [Mettre fin aux instances Amazon EC2](#).
- Vous ne pouvez pas activer la protection contre l'arrêt pour les instances basées sur le stockage d'instances.
- Vous ne pouvez pas activer la protection contre l'arrêt pour les instances Spot.
- L'API Amazon EC2 suit un modèle de cohérence éventuel lorsque vous activez ou désactivez la protection contre l'arrêt. Cela signifie que le résultat de l'exécution de commandes pour définir

l'attribut de protection contre l'arrêt peut ne pas être immédiatement visible pour toutes les commandes suivantes que vous exécuterez. Pour plus d'informations, consultez la section [Cohérence éventuelle](#) dans le manuel Amazon EC2 Developer Guide.

Tâches de la protection contre l'arrêt

- [Activer la protection contre l'arrêt d'une instance lors du lancement](#)
- [Activer la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée](#)
- [Désactivez la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée](#)

Activer la protection contre l'arrêt d'une instance lors du lancement

Vous pouvez activer la protection contre l'arrêt d'une instance lors du lancement d'instance à l'aide d'une des méthodes suivantes.

Console

Pour activer la protection contre l'arrêt d'une instance lors du lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sur le tableau de bord, choisissez Lancer une instance.
3. Configurez votre instance dans le [nouvel assistant de lancement d'instance](#).
4. Dans l'assistant, activez la protection contre l'arrêt en choisissant Activer pour Protection contre l'arrêt sous Détails avancés.

AWS CLI

Pour activer la protection contre l'arrêt d'une instance lors du lancement

Utilisez la AWS CLI commande [run-instances](#) pour lancer l'instance et spécifiez le `disable-api-stop` paramètre.

```
aws ec2 run-instances \  
  --image-id ami-a1b2c3d4e5example \  
  --instance-type t3.micro \  
  --key-name MyKeyPair \  
  --disable-api-stop \  
  ...
```

Activer la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

Vous pouvez activer la protection contre l'arrêt d'une instance lorsque l'instance est en cours d'exécution ou est arrêtée à l'aide d'une des méthodes suivantes.

Console

Pour activer la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, sélectionnez instances.
3. Sélectionnez l'instance, puis cliquez sur Actions>Paramètres de l'instance>Modifier la protection contre l'arrêt.
4. Cochez la case Enable (Activer), puis choisissez Save (Enregistrer).

AWS CLI

Pour activer la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

Utilisez la AWS CLI commande [modify-instance-attribute](#) et spécifiez le paramètre. `disable-api-stop`

```
aws ec2 modify-instance-attribute \  
  --instance-id i-1234567890abcdef0 \  
  --disable-api-stop
```

Désactivez la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

Vous pouvez désactiver la protection contre l'arrêt d'une instance pour une instance en cours d'exécution ou arrêtée à l'aide d'une des méthodes suivantes.

Console

Pour désactiver la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, sélectionnez instances.
3. Sélectionnez l'instance, puis cliquez sur Actions, Instance Settings (Paramètres de l'instance) et Change stop protection (Modifier la protection contre l'arrêt).

4. Décochez la case Enable (Activer), puis choisissez Save (Enregistrer).

AWS CLI

Pour désactiver la protection contre l'arrêt d'une instance en cours d'exécution ou arrêtée

Utilisez la AWS CLI commande [modify-instance-attribute](#) et spécifiez le paramètre `no-disable-api-stop`

```
aws ec2 modify-instance-attribute \  
  --instance-id i-1234567890abcdef0 \  
  --no-disable-api-stop
```

Hibernez votre instance Amazon EC2

Lorsque vous mettez une instance en veille prolongée, Amazon EC2 indique au système d'exploitation de procéder à la mise en veille prolongée (suspend-to-disk). La mise en veille prolongée enregistre le contenu de la mémoire (RAM) de l'instance sur votre volume racine Amazon Elastic Block Store (Amazon EBS). Amazon EC2 conserve le volume racine EBS de l'instance et les volumes de données EBS attachés. Lorsque votre instance est démarrée :

- Le volume racine EBS est restauré à l'état précédent.
- Le contenu de la mémoire RAM est chargé à nouveau.
- Les processus qui s'exécutaient précédemment sur l'instance reprennent.
- Les volumes de données précédemment attachés sont attachés à nouveau et l'instance conserve son ID d'instance.

Vous pouvez mettre une instance en veille prolongée uniquement si celle-ci est [activée pour la mise en veille prolongée](#) et si elle répond aux [prérequis de mise en veille prolongée](#).

Si les actions d'amorçage d'une instance ou d'une application et de création d'une empreinte mémoire afin de devenir complètement productive prennent du temps, vous pouvez utiliser la mise en veille prolongée pour préchauffer l'instance. Pour préchauffer l'instance, vous :

1. La lancez avec la mise en veille prolongée activée.
2. La placez dans l'état souhaité.

3. Mettez-la en veille prolongée afin qu'elle soit prête à reprendre à l'état désiré lorsque cela est nécessaire.

Vous ne payez ni l'utilisation d'une instance mise en veille de manière prolongée lorsque cette dernière est à l'état `stopped`, ni le transfert de données lorsque le contenu de la mémoire RAM est transféré vers le volume racine EBS. Vous payez le stockage de tout volume EBS, y compris le stockage du contenu de la mémoire RAM.

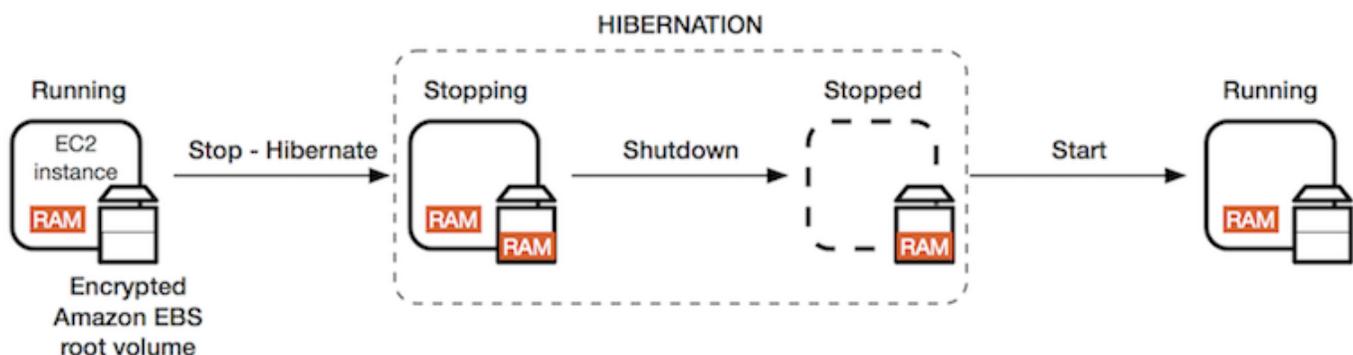
Si vous n'avez plus besoin d'une instance, vous pouvez la résilier à tout moment, y compris quand elle est à un état `stopped` (en veille prolongée). Pour plus d'informations, consultez [Mettre fin aux instances Amazon EC2](#).

Table des matières

- [Comment fonctionne l'hibernation des instances Amazon EC2](#)
- [Conditions préalables à l'hibernation des instances Amazon EC2](#)
- [Configuration d'une AMI Linux pour prendre en charge l'hibernation](#)
- [Activer l'hibernation pour une instance Amazon EC2](#)
- [Désactiver KASLR sur une instance \(Ubuntu uniquement\)](#)
- [Mettre en veille prolongée une instance Amazon EC2](#)
- [Démarez une instance Amazon EC2 mise en veille prolongée](#)
- [Résoudre les problèmes liés à l'hibernation des instances Amazon EC2](#)

Comment fonctionne l'hibernation des instances Amazon EC2

Le schéma suivant présente un aperçu de base du processus d'hibernation pour les instances EC2.



Que se passe-t-il lorsque vous mettez une instance en veille prolongée

Lorsque vous mettez une instance en veille prolongée, voici ce qui se produit :

- L'instance passe à l'état `stopping`. Amazon EC2 indique au système d'exploitation de réaliser la mise en veille prolongée (`suspend-to-disk`). La mise en veille prolongée fige tous les processus, enregistre le contenu de la mémoire RAM sur le volume racine EBS, puis exécute un arrêt normal.
- Lorsque l'arrêt est terminé, l'instance passe à l'état `stopped`.
- Les volumes EBS restent attachés à l'instance et leurs données persistent, y compris le contenu enregistré de la mémoire RAM.
- Tous les volumes de stockage d'instance Amazon EC2 restent attachés à l'instance, mais les données des volumes de stockage d'instances sont perdues.
- Lorsque votre instance se trouve dans l'état `stopped`, vous pouvez modifier certains attributs de l'instance, y compris le type ou la taille d'instance.
- L'instance est généralement migrée vers un nouvel ordinateur hôte sous-jacent lorsqu'elle démarre. Cela se produit également lorsque vous arrêtez et démarrez une instance.
- Lorsque l'instance est démarrée, celle-ci démarre et le système d'exploitation lit le contenu de la mémoire RAM depuis le volume racine EBS avant de « défiger » les processus pour qu'ils reprennent leur état.
- L'instance conserve ses adresses IPv4 privées, ainsi que les adresses IPv6. Lorsque l'instance est démarrée, elle continue de conserver ses adresses IPv4 privées et toutes les adresses IPv6.
- Amazon EC2 publie l'adresse IPv4 publique. Lorsque l'instance est démarrée, Amazon EC2 attribue une nouvelle adresse IPv4 publique à l'instance.
- L'instance conserve les adresses IP Elastic qui lui sont associées. Les adresses IP Elastic qui sont associées à une instance mise en veille prolongée vous seront facturées.

Pour plus d'informations sur les différences entre la mise en veille prolongée, et le redémarrage, l'arrêt et la résiliation, consultez [Différences entre redémarrage, arrêt, mise en veille prolongée et résiliation](#).

Limites

- Lorsque vous mettez en veille une instance, les données contenues sur les volumes de stockage d'instances sont perdues.
- (Instances Linux) Vous ne pouvez pas mettre en veille prolongée une instance Linux qui possède plus de 150 Go de RAM.

- (Instances Windows) Vous ne pouvez pas mettre en veille prolongée une instance Windows qui possède plus de 16 Go de RAM.
- Si vous créez un instantané ou une AMI à partir d'une instance qui est mise en veille prolongée ou dont la mise en veille prolongée est activée, il se peut que vous ne puissiez pas vous connecter à l'instance qui est lancée à partir de l'AMI ou d'une AMI créée à partir de l'instantané
- (Instances Spot uniquement) Si Amazon EC2 met votre instance Spot en veille prolongée, seul Amazon EC2 peut relancer votre instance. Si vous mettez votre instance Spot en veille prolongée ([mise en veille prolongée à l'initiative de l'utilisateur](#)), vous pouvez la relancer. Une instance Spot mise en veille prolongée ne peut être relancée que si la capacité est disponible et si le prix Spot est inférieur ou égal au prix maximum spécifié.
- Vous ne pouvez pas mettre en veille prolongée une instance faisant partie d'un groupe Auto Scaling ou utilisée par Amazon ECS. Si votre instance est dans un groupe Auto Scaling et que vous essayez de la mettre en veille prolongée, le service Amazon EC2 Auto Scaling marque l'instance arrêtée comme étant non saine, et peut la résilier et lancer une instance de remplacement. Pour plus d'informations, consultez [la section Contrôles de santé des instances d'un groupe Auto Scaling](#) dans le manuel Amazon EC2 Auto Scaling User Guide.
- [Vous ne pouvez pas mettre en veille prolongée une instance configurée pour démarrer en mode UEFI lorsque le démarrage sécurisé UEFI est activé.](#)
- Si vous mettez en veille prolongée une instance qui a été lancée dans une Réserve de capacité, la Réserve de capacité ne garantit pas que l'instance mise en veille prolongée peut reprendre après avoir essayé de la démarrer.
- Vous ne pouvez pas mettre en veille prolongée une instance qui utilise une version du noyau inférieure à 5.10 si le mode FIPS (Federal Information Processing Standard) est activé.
- Nous ne prenons pas en charge la conservation d'une instance mise en veille prolongée au-delà de 60 jours. Pour conserver l'instance mise en veille prolongée au-delà de 60 jours, vous devez la démarrer, l'arrêter, puis la démarrer.
- Nous mettons à jour en permanence notre plateforme avec des mises à niveau et des correctifs de sécurité qui peuvent être en conflit avec des instances mises en veille prolongée existantes. Nous vous avertissons des mises à niveau critiques qui nécessitent un démarrage des instances mises en veille prolongée pour que nous puissions effectuer un arrêt ou un redémarrage afin d'appliquer les mises à niveau et les correctifs de sécurité requis.

Considérations relatives à la mise en veille prolongée d'une instance Spot

- Si vous mettez votre instance Spot en veille prolongée, vous pouvez la redémarrer à condition que la capacité soit disponible et que le prix Spot soit inférieur ou égal au prix maximum spécifié.
- Si Amazon EC2 met en veille prolongée votre instance Spot :
 - Seul Amazon EC2 peut relancer votre instance.
 - Amazon EC2 relance l'instance Spot mise en veille prolongée lorsque la capacité est disponible, avec un prix Spot inférieur ou égal au prix maximum spécifié.
 - Avant qu'Amazon EC2 ne mette en veille prolongée votre instance Spot, vous recevrez un avis d'interruption deux minutes avant le début de la mise en veille prolongée.

Pour plus d'informations, consultez [Interruptions d'instance Spot](#).

- Vous pouvez activer la mise en veille prolongée d'une instance Spot de plusieurs manières. Pour plus d'informations, consultez [Spécifier le comportement d'interruption](#).

Conditions préalables à l'hibernation des instances Amazon EC2

Vous pouvez activer la prise en charge de l'hibernation pour une instance à la demande ou une instance ponctuelle lorsque vous la lancez. Vous ne pouvez pas activer l'hibernation sur une instance existante, qu'elle soit en cours d'exécution ou arrêtée. Pour plus d'informations, consultez [Activer l'hibernation de l'instance](#).

Exigences relatives à la mise en veille prolongée d'une instance

- [Régions AWS](#)
- [AMI](#)
- [Familles d'instances](#)
- [Taille de mémoire RAM d'instance](#)
- [Type de volume racine](#)
- [Taille du volume racine](#)
- [Chiffrement du volume racine](#)
- [Type de volume EBS](#)
- [Demandes d'instance Spot](#)

Régions AWS

Vous pouvez utiliser l'hibernation avec toutes Régions AWS les instances.

AMI

Vous devez utiliser une AMI HVM qui prend en charge l'hibernation. Les AMI suivantes prennent en charge l'hibernation :

AMI Linux

- AMI d'AL2023 publiée le 20 septembre 2023 ou version ultérieure
- AMI Amazon Linux 2 publiée le 29 août 2019 ou version ultérieure
- AMI Amazon Linux de mars 2018 publiée le 16 novembre 2018 ou version ultérieure
- AMI CentOS version 8* ¹ ([Configuration supplémentaire](#) obligatoire)
- AMI Fedora version 34 ou ultérieure* ¹ ([Configuration supplémentaire](#) obligatoire)
- AMI Red Hat Enterprise Linux (RHEL) 9 ¹ ([Configuration supplémentaire](#) obligatoire)
- AMI Red Hat Enterprise Linux (RHEL) 8 ¹ ([Configuration supplémentaire](#) obligatoire)
- AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish) publiée avec le numéro de série 20230303 ou version ultérieure ²
- AMI Ubuntu 20.04 LTS (Focal Fossa) publiée avec le numéro de série 20210820 ou ultérieur ²
- AMI Ubuntu 18.04 LTS (Bionic Beaver) publiée avec le numéro de série 20190722.1 ou version ultérieure ^{2 4}
- AMI Ubuntu 16.04 LTS (Xenial Xerus) ^{2 3 4} ([Configuration supplémentaire](#) obligatoire)

¹ Pour CentOS, Fedora et Red Hat Enterprise Linux, la mise en veille prolongée n'est prise en charge que sur les instances Nitro.

² Nous recommandons de désactiver KASLR sur les instances exécutant Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver) et Ubuntu 16.04 LTS (Xenial Xerus). Pour plus d'informations, consultez [Désactiver KASLR sur une instance \(Ubuntu uniquement\)](#).

³ Pour l'AMI Ubuntu 16.04 LTS (Xenial Xerus), la mise en veille prolongée n'est pas prise en charge sur les types d'instance t3.nano. Aucun correctif ne sera disponible, car Ubuntu (Xenial Xerus) a

mis fin au support en avril 2021. Si vous voulez utiliser les types d'instance t3 . nano, nous vous recommandons une mise à niveau vers l'AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa) ou l'AMI Ubuntu 18.04 LTS (Bionic Beaver).

⁴ La prise en charge d'Ubuntu 18.04 LTS (Bionic Beaver) et Ubuntu 16.04 LTS (Xenial Xerus) est arrivée à son terme.

Pour configurer votre propre AMI afin de prendre en charge la mise en veille prolongée, consultez [Configuration d'une AMI Linux pour prendre en charge l'hibernation](#).

La prise en charge d'autres versions d'Ubuntu et d'autres systèmes d'exploitation sera bientôt disponible.

AMI Windows

- AMI Windows Server 2022 publiée le 13/09/2023 ou version ultérieure
- AMI Windows Server 2019 publiée le 11 septembre 2019 ou version ultérieure.
- AMI Windows Server 2016 publiée le 11 septembre 2019 ou version ultérieure.
- AMI Windows Server 2012 R2 publiée le 11 septembre 2019 ou version ultérieure.
- AMI Windows Server 2012 publiée le 11 septembre 2019 ou version ultérieure.

Familles d'instances

Vous devez utiliser une famille d'instances qui prend en charge l'hibernation.

- Usage général : M3, M4, M5, M5a, M5ad, M5d, M6i, M6id, M7i, M7i-Flex, T2, T3, T3a
- Optimisé pour le calcul : C3, C4, C5, C5d, C6i, C6id, C7a, C7i, C7i-Flex
- Mémoire optimisée : R3, R4, R5, R5a, R5ad, R5d, R7a, R7i, R7iz
- Stockage optimisé : I3, i3EN

Instances Nitro : les instances bare metal ne sont pas prises en charge.

Pour consulter les types d'instance disponibles qui prennent en charge la mise en veille prolongée dans une région spécifique

Les types d'instance disponibles varient selon la région. Pour consulter les types d'instance disponibles qui prennent en charge la mise en veille prolongée dans une Région, utilisez la commande [describe-instance-types](#) (décrire le type d'instance) avec le paramètre `--region`.

Incluez le paramètre `--filters` pour étendre les résultats aux types d'instance qui prennent en charge la mise en veille prolongée et le paramètre `--query` pour étendre la sortie à la valeur de `InstanceType`.

```
aws ec2 describe-instance-types --filters Name=hibernation-supported,Values=true --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Exemple de sortie

```
c3.2xlarge  
c3.4xlarge  
c3.8xlarge  
c3.large  
c3.xlarge  
c4.2xlarge  
c4.4xlarge  
c4.8xlarge  
...
```

Taille de mémoire RAM d'instance

Instances Linux : leur taille doit être inférieure à 150 Go.

Instances Windows : jusqu'à 16 Go. Pour mettre en veille prolongée une instance Windows T3 ou T3a, nous recommandons au moins 1 Go de RAM.

Type de volume racine

Le volume racine doit être un volume EBS, et non un volume de stockage d'instance.

Taille du volume racine

Le volume racine doit être suffisamment grand pour stocker le contenu de la RAM et s'adapter à l'utilisation prévue, par exemple, du système d'exploitation ou des applications. Si vous activez la mise en veille prolongée, un espace est alloué sur le volume racine au lancement pour stocker la mémoire RAM.

Chiffrement du volume racine

Le volume racine doit être chiffré pour garantir la protection du contenu sensible qui se trouve en mémoire au moment de l'hibernation. Lorsque les données de la mémoire RAM sont transférées vers

le volume racine EBS, celui-ci est toujours chiffré. Le chiffrement du volume racine est appliqué au lancement de l'instance.

L'une des trois options suivantes permet de s'assurer que le volume racine est une volume EBS chiffré :

- EBS encryption by default (Chiffrement EBS par défaut) : vous pouvez activer le chiffrement EBS par défaut afin de vous assurer que tous les nouveaux volumes EBS de votre compte AWS sont chiffrés. De cette façon, vous pouvez activer l'hibernation pour vos instances sans spécifier d'intention de chiffrement au moment du lancement de l'instance. Pour plus d'informations, voir [Activer le chiffrement par défaut](#).
- EBS "single-step" encryption (Chiffrement EBS « en une étape ») : vous pouvez lancer des instances EC2 chiffrées basées sur EBS depuis une AMI non chiffrée et activer la mise en veille prolongée en même temps. Pour plus d'informations, consultez [Utiliser le chiffrement avec des AMI basées sur EBS](#).
- Encrypted AMI (AMI chiffrée) : vous pouvez activer le chiffrement EBS en utilisant une AMI chiffrée pour lancer votre instance. Si votre AMI ne dispose d'aucun volume racine chiffré, vous pouvez le copier sur le nouvel AMI et demander son chiffrement. Pour plus d'informations, consultez [Chiffrement d'une image non chiffrée pendant la copie](#) et [Copier une AMI](#).

Type de volume EBS

Les volumes EBS doivent utiliser l'un des types de volumes EBS suivants :

- SSD à usage général (gp2 et gp3)
- SSD à IOPS provisionnés (io1 et io2)

Si vous choisissez un type de volume SSD à IOPS provisionnés, vous devez provisionner le volume EBS avec les IOPS appropriées pour obtenir des performances optimales pour la mise en veille prolongée,. Pour plus d'informations, consultez les [types de volumes Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

Demandes d'instance Spot

Pour les instances Spot, les exigences suivantes s'appliquent :

- Le type de la demande d'instance Spot doit être `persistent`.
- Vous ne pouvez pas spécifier de groupe de lancement dans la demande d'instance Spot.

Configuration d'une AMI Linux pour prendre en charge l'hibernation

Les AMI Linux suivantes prennent en charge l'hibernation, mais pour mettre en veille prolongée une instance lancée avec l'une de ces AMI, une configuration supplémentaire est requise avant de pouvoir mettre l'instance en veille prolongée.

Une configuration supplémentaire est requise pour :

- [AMI minimale Amazon Linux 2 publiée le 29 août 2019 ou version ultérieure](#)
- [Amazon Linux 2 publiées avant le 29.08.2019](#)
- [Amazon Linux 2 publiées avant le 16.11.2018](#)
- [CentOS version 8 ou ultérieure](#)
- [Fedora version 34 ou ultérieure](#)
- [Red Hat Enterprise Linux version 8 ou 9](#)
- [Ubuntu 20.04 LTS \(Focal Fossa\) publié avant le numéro de série 20210820](#)
- [Ubuntu 18.04 \(Bionic Beaver\) publié avant le numéro de série 20190722.1](#)
- [Ubuntu 16.04 \(Xenial Xenus\)](#)

Pour plus d'informations, consultez [Mettre à jour le logiciel de l'instance sur votre instance Amazon Linux 2](#).

Aucune configuration supplémentaire n'est requise pour les AMI suivantes car elles sont déjà configurées pour prendre en charge la mise en veille prolongée :

- AMI d'AL2023 publiée le 20 septembre 2023 ou version ultérieure
- AMI complète Amazon Linux 2 publiée le 29 août 2019 ou version ultérieure
- AMI Amazon Linux de mars 2018 publiée le 16 novembre 2018 ou version ultérieure
- AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish) publiée avec le numéro de série 20230303 ou version ultérieure
- AMI Ubuntu 20.04 LTS (Focal Fossa) publiée avec le numéro de série 20210820 ou ultérieur
- AMI Ubuntu 18.04 LTS (Bionic Beaver) publiée avec le numéro de série 20190722.1 ou ultérieur

AMI minimale Amazon Linux 2 publiée le 29 août 2019 ou version ultérieure

Pour configurer une AMI minimale Amazon Linux 2 publiée le 20 août 2019 ou ultérieurement afin de prendre en charge la mise en veille prolongée

1. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Redémarrez le service .

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Amazon Linux 2 publiées avant le 29.08.2019

Pour configurer une AMI Amazon Linux 2 publiée avant le 29.08.2019 afin de prendre en charge la mise en veille prolongée

1. Mettez à jour le noyau vers `4.14.138-114.102` ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

4. Vérifiez que la version du noyau a été mise à jour vers `4.14.138-114.102` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

5. Arrêtez l'instance et créez une AMI. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).

Amazon Linux 2 publiées avant le 16.11.2018

Pour configurer une AMI Amazon Linux 2 publiée avant le 16.11.2018 afin de prendre en charge la mise en veille prolongée

1. Mettez à jour le noyau vers 4.14.77-70.59 ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

4. Vérifiez que la version du noyau est mise à jour vers 4.14.77-70.59 ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

5. Arrêtez l'instance et créez une AMI. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).

CentOS version 8 ou ultérieure

Pour configurer une AMI CentOS version 8 ou ultérieure afin de prendre en charge la mise en veille prolongée

1. Mettez à jour le noyau vers 4.18.0-305.7.1.el8_4.x86_64 ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le référentiel Fedora Extra Packages for Enterprise Linux (EPEL).

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Activez l'agent de mise en veille prolongée pour démarrer au démarrage.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

6. Vérifiez que la version du noyau a été mise à jour vers 4.18.0-305.7.1.el8_4.x86_64 ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Fedora version 34 ou ultérieure

Pour configurer une AMI Fedora version 34 ou ultérieure afin de prendre en charge la mise en veille prolongée

1. Mettez à jour le noyau vers 5.12.10-300.fc34.x86_64 ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Activez l'agent de mise en veille prolongée pour démarrer au démarrage.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

5. Vérifiez que la version du noyau a été mise à jour vers 5.12.10-300.fc34.x86_64 ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux version 8 ou 9

Pour configurer une AMI Red Hat Enterprise Linux version 8 ou 9 afin de prendre en charge la mise en veille prolongée

1. Mettez à jour le noyau vers `4.18.0-305.7.1.el8_4.x86_64` ou version ultérieure.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installez le référentiel Fedora Extra Packages for Enterprise Linux (EPEL).

RHEL version 8 :

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

RHEL version 9 :

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

3. Installez le package `ec2-hibinit-agent` à partir des référentiels.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Activez l'agent de mise en veille prolongée pour démarrer au démarrage.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

6. Vérifiez que la version du noyau a été mise à jour vers `4.18.0-305.7.1.el8_4.x86_64` ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 LTS (Focal Fossa) publié avant le numéro de série 20210820

Pour configurer une AMI Ubuntu LTS 20.04 (Focal Fossa) publiée avant le numéro de série 20210820 afin de prendre en charge la mise en veille prolongée

1. Mettez à jour le linux-aws-kernel vers 5.8.0-1038.40 ou une version ultérieure, et grub2 vers 2.04-1ubuntu26.13 ou une version ultérieure.

```
[ec2-user ~]$ sudo apt update  
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

3. Vérifiez que la version du noyau a été mise à jour vers 5.8.0-1038.40 ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

4. Vérifiez que la version de grub2 a été mise à jour vers 2.04-1ubuntu26.13 ou une version ultérieure.

```
[ec2-user ~]$ dpkg --get-selections | grep grub2-common
```

Ubuntu 18.04 (Bionic Beaver) publié avant le numéro de série 20190722.1

Pour configurer une AMI Ubuntu LTS 18.04 publiée avant le numéro de série 20190722.1 afin de prendre en charge la mise en veille prolongée

1. Mettez à jour le noyau vers 4.15.0-1044 ou version ultérieure.

```
[ec2-user ~]$ sudo apt update  
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Installez le package ec2-hibinit-agent à partir des référentiels.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

4. Vérifiez que la version du noyau a été mise à jour vers 4.15.0-1044 ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xerus)

Pour configurer Ubuntu 16.04 LTS afin de prendre en charge l'hibernation, vous devez installer le package du linux-aws-hwe noyau version 4.15.0-1058-aws ou ultérieure et l'agent ec2-hibinit-agent.

Important

Le package noyau linux-aws-hwe est pris en charge par Canonical. La prise en charge standard d'Ubuntu 16.04 LTS a pris fin en avril 2021 et le package ne reçoit plus de mises à jour régulières. Il recevra toutefois des mises à jour de sécurité supplémentaires jusqu'à ce que la prise en charge de la maintenance de sécurité étendue prenne fin en 2024. Pour plus d'informations, consultez [Amazon EC2 Hibernation for Ubuntu 16.04 LTS now available](#) sur le blog Canonical Ubuntu.

Nous vous recommandons une mise à niveau vers l'AMI Ubuntu 20.04 LTS (Focal Fossa) ou l'AMI Ubuntu 18.04 LTS (Bionic Beaver).

Pour configurer une AMI Ubuntu 16.04 LTS afin de prendre en charge la mise en veille prolongée

1. Mettez à jour le noyau vers 4.15.0-1058-aws ou version ultérieure.

```
[ec2-user ~]$ sudo apt update  
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Installez le package ec2-hibinit-agent à partir des référentiels.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

4. Vérifiez que la version du noyau a été mise à jour vers 4.15.0-1058-aws ou une version ultérieure.

```
[ec2-user ~]$ uname -a
```

Activer l'hibernation pour une instance Amazon EC2

Pour mettre en veille prolongée une instance, vous devez d'abord l'activer pour la mise en veille prolongée lors du lancement de l'instance.

Important

Vous ne pouvez pas activer ou désactiver la mise en veille prolongée pour une instance après son lancement.

Rubriques

- [Activer la mise en veille prolongée pour les instances à la demande](#)
- [Activer la mise en veille prolongée pour les instances Spot](#)
- [Voir si une instance est activée pour la mise en veille prolongée](#)

Activer la mise en veille prolongée pour les instances à la demande

Utilisez l'une des méthodes suivantes pour activer la mise en veille prolongée pour vos instances à la demande.

New console

Pour activer la mise en veille prolongée pour une instance à la demande

1. Suivez la procédure pour [lancer une instance](#), mais ne lancez l'instance qu'après avoir effectué les étapes suivantes pour activer l'hibernation.
2. Pour activer l'hibernation, configurez les champs suivants dans l'assistant de lancement de l'instance :

- a. Sous Application and OS Images (Amazon Machine Image) (Images d'applications et de systèmes d'exploitation), sélectionnez une AMI qui prend en charge la mise en veille prolongée. Pour plus d'informations, consultez [AMI](#).
- b. Pour Instance type (Type d'Instance), sélectionnez un type d'instance pris en charge. Pour plus d'informations, consultez [Familles d'instances](#).
- c. Sous Configure storage (Configurer le stockage), choisissez Advanced (Avancé) (à droite), et spécifiez les informations suivantes pour le volume racine :
 - Pour Taille (Go), saisissez la taille du volume EBS racine. Le volume doit être suffisamment grand pour stocker le contenu de la mémoire RAM et prendre en compte l'utilisation que vous prévoyez.
 - Sous Volume type (Type de volume), sélectionnez un type de volume EBS pris en charge : SSD à usage général (gp2 et gp3) ou SSD IOPS provisionnés (io1 et io2).
 - Pour Encrypted (Chiffré), choisissez Yes (Oui). Si vous avez activé le chiffrement par défaut dans cette AWS région, l'option Oui est sélectionnée.
 - Pour KMS key (Clé KMS), sélectionnez la clé de chiffrement pour le volume. Si vous avez activé le chiffrement par défaut dans cette AWS région, la clé de chiffrement par défaut est sélectionnée.

Pour plus d'informations sur les prérequis relatifs au volume racine, consultez [Conditions préalables à l'hibernation des instances Amazon EC2](#).

- d. Développez Advanced details (Détails avancés), et pour Stop - Hibernate behavior (Arrêt – Comportement de mise en veille prolongée), choisissez Enable (Activer).
3. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Old console

Pour activer la mise en veille prolongée pour une instance à la demande

1. Suivez la procédure [Lancer une instance à l'aide de l'ancien assistant de lancement d'instance](#).

2. Sur la page Sélection d'une Amazon Machine Image (AMI), sélectionnez une AMI qui prend en charge la mise en veille prolongée. Pour plus d'informations sur les AMI supportées, consultez [Conditions préalables à l'hibernation des instances Amazon EC2](#).
3. Sur la page Choisir un type d'instance, sélectionnez un type d'instance pris en charge, puis choisissez Suivant : Configurer les détails de l'instance. Pour plus d'informations sur les types d'instance pris en charge, consultez [Conditions préalables à l'hibernation des instances Amazon EC2](#).
4. Sur la page Configurer les détails de l'instance, pour Stop - Hibernate Behavior (Arrêter - Comportement de mise en veille prolongée), cochez la case Enable hibernation as an additional stop behavior (Activer la mise en veille prolongée comme comportement d'arrêt supplémentaire).
5. Dans la page Ajouter un stockage pour le volume racine, spécifiez les informations suivantes :
 - Pour Taille (Go), saisissez la taille du volume EBS racine. Le volume doit être suffisamment grand pour stocker le contenu de la mémoire RAM et prendre en compte l'utilisation que vous prévoyez.
 - Pour Type de volume, sélectionnez un type de volume EBS pris en charge (SSD à usage général (gp2 et gp3) ou SSD IOPS provisionnés (io1 et io2)).
 - Pour Chiffrement, sélectionnez la clé de chiffrement du volume. Si vous avez activé le chiffrement par défaut dans cette AWS région, la clé de chiffrement par défaut est sélectionnée.

Pour plus d'informations sur les prérequis relatifs au volume racine, consultez [Conditions préalables à l'hibernation des instances Amazon EC2](#).

6. Continuez comme indiqué par l'assistant. Lorsque vous avez terminé de vérifier vos options sur la page Examiner le lancement de l'instance, choisissez Lancer. Pour plus d'informations, consultez [Lancer une instance à l'aide de l'ancien assistant de lancement d'instance](#).

AWS CLI

Pour activer la mise en veille prolongée pour une instance à la demande

Utilisez la commande [run-instances](#) pour lancer une instance. Spécifiez les paramètres du volume racine EBS à l'aide du paramètre `--block-device-mappings file://mapping.json`

et activez la mise en veille prolongée à l'aide du paramètre `--hibernation-options Configured=true`.

```
aws ec2 run-instances \  
  --image-id ami-0abcdef1234567890 \  
  --instance-type m5.large \  
  --block-device-mappings file://mapping.json \  
  --hibernation-options Configured=true \  
  --count 1 \  
  --key-name MyKeyPair
```

Spécifiez les éléments suivants dans `mapping.json`.

```
[  
  {  
    "DeviceName": "/dev/xvda",  
    "Ebs": {  
      "VolumeSize": 30,  
      "VolumeType": "gp2",  
      "Encrypted": true  
    }  
  }  
]
```

Note

La valeur de `DeviceName` doit correspondre au nom du périphérique racine associé à l'AMI. Pour trouver le nom du périphérique racine, utilisez la commande [describe-images](#) (décrire les images).

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Si vous avez activé le chiffrement par défaut dans cette AWS région, vous pouvez l'omettre `"Encrypted": true`.

PowerShell

Pour activer l'hibernation pour une instance à la demande à l'aide du AWS Tools for Windows PowerShell

Utilisez la [New-EC2Instance](#) commande pour lancer une instance. Spécifiez le volume racine EBS en définissant d'abord le mappage au périphérique de stockage en mode bloc, puis en l'ajoutant à la commande à l'aide du paramètre `-BlockDeviceMappings`. Activez la mise en veille prolongée à l'aide du paramètre `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair
```

Note

La valeur de `DeviceName` doit correspondre au nom du périphérique racine associé à l'AMI. Pour trouver le nom du périphérique racine, utilisez la [Get-EC2Image](#) commande.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Si vous avez activé le chiffrement par défaut dans cette AWS région, vous pouvez omettre le mappage `Encrypted = $true` des périphériques par blocs.

Activer la mise en veille prolongée pour les instances Spot

Utilisez l'une des méthodes suivantes pour activer la mise en veille prolongée pour vos instances Spot. Pour plus d'informations sur la mise en veille prolongée des instances Spot en cas d'interruption, consultez la rubrique [Interruptions d'instance Spot](#).

Console

Vous pouvez utiliser l'assistant de lancement d'instance de la console Amazon EC2 pour activer la mise en veille prolongée pour une instance Spot.

Pour activer la mise en veille prolongée pour une instance Spot

1. Suivez la procédure pour [demande une instance Spot à l'aide de l'assistant de lancement d'instance](#), mais ne lancez l'instance qu'après avoir effectué les étapes suivantes pour activer la mise en veille prolongée.
2. Pour activer l'hibernation, configurez les champs suivants dans l'assistant de lancement de l'instance :
 - a. Sous Application and OS Images (Amazon Machine Image) (Images d'applications et de systèmes d'exploitation), sélectionnez une AMI qui prend en charge la mise en veille prolongée. Pour plus d'informations, consultez [AMI](#).
 - b. Pour Instance type (Type d'Instance), sélectionnez un type d'instance pris en charge. Pour plus d'informations, consultez [Familles d'instances](#).
 - c. Sous Configure storage (Configurer le stockage), choisissez Advanced (Avancé) (à droite), et spécifiez les informations suivantes pour le volume racine :
 - Pour Taille (Go), saisissez la taille du volume EBS racine. Le volume doit être suffisamment grand pour stocker le contenu de la mémoire RAM et prendre en compte l'utilisation que vous prévoyez.
 - Sous Volume type (Type de volume), sélectionnez un type de volume EBS pris en charge : SSD à usage général (gp2 et gp3) ou SSD IOPS provisionnés (io1 et io2).
 - Pour Encrypted (Chiffré), choisissez Yes (Oui). Si vous avez activé le chiffrement par défaut dans cette AWS région, l'option Oui est sélectionnée.
 - Pour KMS key (Clé KMS), sélectionnez la clé de chiffrement pour le volume. Si vous avez activé le chiffrement par défaut dans cette AWS région, la clé de chiffrement par défaut est sélectionnée.

Pour plus d'informations sur les prérequis relatifs au volume racine, consultez [Conditions préalables à l'hibernation des instances Amazon EC2](#).

- d. Développez Détails avancés et, en plus des champs de configuration d'une instance Spot, procédez comme suit :

- i. Pour Type de demande, choisissez Persistente.
 - ii. Pour Comportement d'interruption, choisissez Mise en veille prolongée. Sinon, pour Comportement d'arrêt - mise en veille prolongée, choisissez Activer. Les deux champs activent la mise en veille prolongée sur votre instance Spot. Vous devez uniquement configurer l'un de ces champs.
3. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

AWS CLI

Vous pouvez activer la mise en veille prolongée pour une instance Spot à l'aide de la commande de l' AWS CLI [run-instances](#).

Pour activer la mise en veille prolongée pour une instance Spot à l'aide du paramètre **hibernation-options**

Utilisez la commande [run-instances](#) pour demander une instance Spot. Spécifiez les paramètres du volume racine EBS à l'aide du paramètre `--block-device-mappings file://mapping.json` et activez la mise en veille prolongée à l'aide du paramètre `--hibernation-options Configured=true`. Le type de la demande Spot (`SpotInstanceType`) doit être `persistent`.

```
aws ec2 run-instances \  
  --image-id ami-0abcdef1234567890 \  
  --instance-type c4.xlarge \  
  --block-device-mappings file://mapping.json \  
  --hibernation-options Configured=true \  
  --count 1 \  
  --key-name MyKeyPair \  
  --instance-market-options \  
    { \  
      "MarketType":"spot", \  
      "SpotOptions":{ \  
        "MaxPrice":"1", \  
        "SpotInstanceType":"persistent" \  
      } \  
    } \  
  }
```

Spécifiez les paramètres du volume racine EBS dans `mapping.json` comme suit.

```
[
  {
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 30,
      "VolumeType": "gp2",
      "Encrypted": true
    }
  }
]
```

Note

La valeur de `DeviceName` doit correspondre au nom du périphérique racine associé à l'AMI. Pour trouver le nom du périphérique racine, utilisez la commande [describe-images](#) (décrire les images).

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Si vous avez activé le chiffrement par défaut dans cette AWS région, vous pouvez omettre `"Encrypted": true`.

PowerShell

Pour activer l'hibernation d'une instance Spot à l'aide du AWS Tools for Windows PowerShell

Utilisez la [New-EC2Instance](#) commande pour demander une instance Spot. Spécifiez le volume racine EBS en définissant d'abord le mappage au périphérique de stockage en mode bloc, puis en l'ajoutant à la commande à l'aide du paramètre `-BlockDeviceMappings`. Activez la mise en veille prolongée à l'aide du paramètre `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true
```

```
PS C:\> New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair `
    -InstanceMarketOption @(
        MarketType = spot;
        SpotOptions @{
            MaxPrice = 1;
            SpotInstanceType = persistent}
    )
```

Note

La valeur de DeviceName doit correspondre au nom du périphérique racine associé à l'AMI. Pour trouver le nom du périphérique racine, utilisez la [Get-EC2Image](#) commande.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Si vous avez activé le chiffrement par défaut dans cette AWS région, vous pouvez omettre le mappage Encrypted = \$true des périphériques par blocs.

Vous pouvez activer la mise en veille prolongée d'une instance Spot de plusieurs manières. Pour plus d'informations, consultez [Spécifier le comportement d'interruption](#).

Voir si une instance est activée pour la mise en veille prolongée

Utilisez les instructions suivantes pour voir si une instance est activée pour la mise en veille prolongée.

Console

Pour voir si une instance est activée pour la mise en veille prolongée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.

- Sélectionnez l'instance et, sous l'onglet Détails de la section Détails de l'instance, inspectez le comportement Stop-hibernate. La valeur Enabled (Activé) indique que l'instance est activée pour la mise en veille prolongée.

AWS CLI

Pour voir si une instance est activée pour la mise en veille prolongée

Utilisez la commande [describe-instances](#) et spécifiez le paramètre `--filters` `"Name=hibernation-options.configured,Values=true"` pour filtrer les instances qui sont activées pour la mise en veille prolongée.

```
aws ec2 describe-instances \  
  --filters "Name=hibernation-options.configured,Values=true"
```

Le champ suivant dans le résultat indique que l'instance est activée pour la mise en veille prolongée.

```
"HibernationOptions": {  
  "Configured": true  
}
```

PowerShell

Pour voir si une instance est activée pour la mise en veille prolongée à l'aide d' AWS Tools for Windows PowerShell

Utilisez la [Get-EC2Instance](#) commande et spécifiez le `-Filter @{ Name="hibernation-options.configured"; Value="true"}` paramètre pour filtrer les instances activées pour l'hibernation.

```
(Get-EC2Instance -Filter @{Name="hibernation-options.configured";  
  Value="true"}).Instances
```

Le résultat répertorie les instances EC2 qui sont activées pour l'hibernation.

Désactiver KASLR sur une instance (Ubuntu uniquement)

Pour exécuter une mise en veille prolongée sur une instance récemment lancée avec Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver) publiée avec le numéro de

série 20190722.1 ou ultérieur ou Ubuntu 20.04 LTS (Focal Fossa) publiée avec le numéro de série 20210820 ou ultérieur, il est recommandé de désactiver KASLR (Kernel Address Space Layout Randomization). Sur Ubuntu 16.04 LTS, Ubuntu 18.04 LTS ou Ubuntu 20.04 LTS, KASLR est activé par défaut.

KASLR est une fonction de sécurité du noyau Linux standard qui permet d'atténuer l'exposition aux vulnérabilités d'accès à la mémoire pas encore découvertes, et leurs ramifications, en randomisant la valeur de l'adresse de base du noyau. En activant KASLR, il est possible que l'instance ne reprenne pas son exécution après sa mise en veille prolongée.

Pour en savoir plus sur KASLR, consultez la page relative aux [fonctionnalités d'Ubuntu](#).

Pour désactiver KASLR sur une instance lancée avec Ubuntu

1. Connectez-vous à votre instance à l'aide de SSH. Pour plus d'informations, consultez [the section called "Connexion à partir de macOS ou Linux avec SSH"](#).
2. Ouvrez le fichier `/etc/default/grub.d/50-cloudimg-settings.cfg` dans l'éditeur de votre choix. Éditez la ligne `GRUB_CMDLINE_LINUX_DEFAULT` de sorte à ajouter l'option `nokaslr` à la fin de la ligne, comme illustré dans l'exemple suivant.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0  
nvme_core.io_timeout=4294967295 nokaslr"
```

3. Enregistrez le fichier et quittez votre éditeur.
4. Exécutez la commande suivante pour recréer la configuration Grub.

```
[ec2-user ~]$ sudo update-grub
```

5. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

6. Exécutez la commande suivante pour confirmer que `nokaslr` a été ajouté.

```
[ec2-user ~]$ cat /proc/cmdline
```

Le résultat de la commande doit inclure l'option `nokaslr`.

Mettre en veille prolongée une instance Amazon EC2

Vous pouvez lancer la mise en veille prolongée sur une instance à la demande ou une instance Spot si l'instance est une instance basée sur EBS, si elle est [activée pour la mise en veille prolongée](#) et si elle répond aux [prérequis de la mise en veille prolongée](#). Si une instance ne peut pas être mise en veille prolongée, un arrêt normal a lieu.

Console

Pour mettre une instance en veille prolongée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance et choisissez État de l'instance, Mettre en veille prolongée les instances. Si Mettre l'instance en veille prolongée est désactivé, l'instance est déjà en veille prolongée ou arrêtée, ou elle ne peut pas être mise en veille prolongée. Pour plus d'informations, consultez [Conditions préalables à l'hibernation des instances Amazon EC2](#).
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Mettre en veille prolongée. La mise en veille prolongée de l'instance peut prendre quelques minutes. L'état de l'instance passe d'abord à Stopping(En cours d'arrêt), puis passe à Stopped (Arrêté(e)) lorsque l'instance est mise en veille prolongée.

AWS CLI

Pour mettre en veille prolongée une instance basée sur EBS

Utilisez la commande [stop-instances](#) et spécifiez le paramètre `--hibernate`.

```
aws ec2 stop-instances \  
  --instance-ids i-1234567890abcdef0 \  
  --hibernate
```

PowerShell

Pour mettre en veille prolongée une instance à l'aide du AWS Tools for Windows PowerShell

Utilisez la [Stop-EC2Instance](#) commande et spécifiez le `-Hibernate $true` paramètre.

```
Stop-EC2Instance `
```

```
-InstanceId i-1234567890abcdef0 `
-Hibernate $true
```

Console

Pour voir si la mise en veille prolongée est initiée sur une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et, sous l'onglet Détails de la section Détails de l'instance, vérifiez la valeur du champ Message de transition d'état.

Client. UserInitiatedMise en veille prolongée : la mise en veille prolongée initiée par l'utilisateur indique que vous avez lancé l'hibernation sur l'instance à la demande ou sur l'instance ponctuelle.

AWS CLI

Pour voir si la mise en veille prolongée est initiée sur une instance

Utilisez la commande [describe-instances](#) et spécifiez le filtre `state-reason-code` pour afficher les instances sur lesquelles la mise en veille prolongée est initiée.

```
aws ec2 describe-instances \
  --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

Le champ suivant dans le résultat indique que la mise en veille prolongée a été initiée sur l'instance à la demande ou sur l'instance Spot.

```
"StateReason": {
  "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

Pour voir si la mise en veille prolongée est initiée sur une instance à l'aide d' AWS Tools for Windows PowerShell

Utilisez la [Get-EC2Instance](#) commande et spécifiez le `state-reason-code` filtre pour voir les instances sur lesquelles l'hibernation a été initiée.

```
Get-EC2Instance `
  -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

Le résultat répertorie les instances EC2 sur lesquelles la mise en veille prolongée a été initiée.

Démarrez une instance Amazon EC2 mise en veille prolongée

Démarrez une instance mise en veille prolongée comme vous le feriez pour une instance arrêtée.

Note

Pour les instances Spot, si Amazon EC2 a mis l'instance en veille prolongée, seul Amazon EC2 peut la relancer. Vous ne pouvez relancer une instance Spot mise en veille prolongée que si vous êtes à l'origine de la mise en veille prolongée. Les instances Spot ne peuvent être relancées que si la capacité est disponible et si le prix Spot est inférieur ou égal au prix maximum spécifié.

Console

Pour démarrer une instance mise en veille prolongée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance mise en veille prolongée et choisissez État de l'instance, Démarrer l'instance. Il peut s'écouler quelques minutes avant que l'instance ne passe à l'état `running`. Pendant ce temps, les [contrôles de statut](#) de l'instance montrent l'instance à un état d'échec jusqu'à ce que l'instance ait démarré.

AWS CLI

Pour démarrer une instance mise en veille prolongée

Utilisez la commande [start-instances](#).

```
aws ec2 start-instances \  
  --instance-ids i-1234567890abcdef0
```

PowerShell

Pour démarrer une instance mise en veille prolongée à l'aide du AWS Tools for Windows PowerShell

Utilisez la commande [Start-EC2Instance](#).

```
Start-EC2Instance \  
  -InstanceId i-1234567890abcdef0
```

Résoudre les problèmes liés à l'hibernation des instances Amazon EC2

Utilisez ces informations pour diagnostiquer et résoudre les problèmes courants que vous pourriez rencontrer lors de la mise en veille prolongée d'une instance.

Problèmes relatifs à la mise en veille prolongée

- [Impossible d'effectuer une mise en veille prolongée immédiatement après le lancement](#)
- [Le passage de stopping à stopped prend du temps et l'état de la mémoire n'est pas restauré après le démarrage](#)
- [Instance « bloquée » dans l'état d'arrêt](#)
- [Impossible de démarrer l'instance Spot immédiatement après la mise en veille prolongée](#)
- [Échec de la reprise des instances Spot](#)

Impossible d'effectuer une mise en veille prolongée immédiatement après le lancement

Si vous essayez de mettre en veille prolongée une instance trop rapidement après l'avoir lancée, vous obtiendrez une erreur.

Vous devez attendre environ deux minutes pour les instances Linux et environ cinq minutes pour les instances Windows après le lancement avant de passer en veille prolongée.

Le passage de **stopping** à **stopped** prend du temps et l'état de la mémoire n'est pas restauré après le démarrage

Si votre instance mise en veille prolongée prend du temps pour passer de l'état `stopping` à `stopped`, et si l'état de la mémoire n'est pas restauré après que vous avez démarré, cela peut indiquer que la mise en veille prolongée n'a pas été configurée correctement.

Instances Linux

Consultez le journal système de l'instance et recherchez les messages liés à la mise en veille prolongée. Pour accéder au journal système, [connectez-vous](#) à l'instance ou utilisez la commande [get-console-output](#). Recherchez les lignes de journal de l'agent `hibinit-agent`. Si les lignes de journal indiquent un échec ou si les lignes de journal sont manquantes, il est probable qu'un échec de la configuration de la mise en veille prolongée au lancement ait eu lieu.

Par exemple, le message suivant indique que le volume racine de l'instance n'est pas suffisamment grand : `hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Si la dernière ligne de journal de `hibinit-agent` est `hibinit-agent: Running: swapoff / swap`, la mise en veille prolongée a été configurée avec succès.

Si vous ne voyez aucun journal issu de ces processus, votre AMI ne prend pas en charge la mise en veille prolongée. Pour plus d'informations sur les AMI supportées, consultez [Conditions préalables à l'hibernation des instances Amazon EC2](#). Si vous avez utilisé votre propre AMI Linux, assurez-vous d'avoir suivi les instructions de [Configuration d'une AMI Linux pour prendre en charge l'hibernation](#).

Windows Server 2016 et versions ultérieures

Consultez le journal de lancement de l'instance EC2 et recherchez les messages liés à la mise en veille prolongée. Pour accéder au journal de lancement de l'instance EC2, [connectez-vous](#) à l'instance et ouvrez le fichier `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` dans un éditeur de texte. Si vous utilisez EC2Launch v2, ouvrez `C:\ProgramData\Amazon\EC2Launch\Log\agent.log`.

Note

Par défaut, Windows masque les fichiers et les dossiers qui se trouvent sous `C:\ProgramData`. Pour afficher les fichiers et les répertoires de lancement de l'instance EC2,

vous devez taper le chemin d'accès dans l'Explorateur Windows ou modifier les propriétés de dossier afin d'afficher les fichiers et les dossiers masqués.

Recherchez les lignes de journal pour la mise en veille prolongée. Si les lignes de journal indiquent un échec ou si les lignes de journal sont manquantes, il est probable qu'un échec de la configuration de la mise en veille prolongée au lancement ait eu lieu.

Par exemple, le message suivant indique que la mise en veille prolongée n'a pas pu être configurée :
Message: Failed to enable hibernation. si le message d'erreur inclut des valeurs ASCII décimales, vous pouvez convertir les valeurs ASCII en texte brut afin de lire le message d'erreur complet.

Si la ligne de journal contient `HibernationEnabled: true`, la mise en veille prolongée a été configurée avec succès.

Windows Server 2012 R2 et versions antérieures

Consultez le journal de configuration de l'instance EC2 et recherchez les messages liés à la mise en veille prolongée. Pour accéder au journal de configuration de l'instance EC2, [connectez-vous](#) à l'instance et ouvrez le fichier `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` dans un éditeur de texte. Recherchez les lignes de journal pour `SetHibernateOnSleep`. Si les lignes de journal indiquent un échec ou si les lignes de journal sont manquantes, il est probable qu'un échec de la configuration de la mise en veille prolongée au lancement ait eu lieu.

Par exemple, le message suivant indique que le volume racine de l'instance n'est pas suffisamment grand :
`SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Si la ligne de journal est `SetHibernateOnSleep: HibernationEnabled: true`, la mise en veille prolongée a été configurée avec succès.

Taille de l'instance Windows

Si vous utilisez une instance Windows T3 ou T3a avec moins de 1 Go de RAM, essayez d'augmenter la taille de l'instance pour qu'elle dispose d'au moins 1 Go de RAM.

Instance « bloquée » dans l'état d'arrêt

Si vous avez mis votre instance en veille prolongée que celle-ci semble « bloquée » à l'état `stopping`, vous pouvez forcer son arrêt. Pour plus d'informations, consultez [Résoudre les problèmes d'arrêt de votre instance](#).

Impossible de démarrer l'instance Spot immédiatement après la mise en veille prolongée

Si vous essayez de démarrer une instance Spot dans les deux minutes suivant sa mise en veille prolongée, le message d'erreur suivant peut s'afficher :

```
You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.
```

Attendez environ deux minutes pour les instances Linux et environ cinq minutes pour les instances Windows, puis réessayez de démarrer l'instance.

Échec de la reprise des instances Spot

Si votre instance Spot a été mise en veille prolongée avec succès, mais qu'elle n'a pas pu reprendre, et qu'elle a été redémarrée (un nouveau redémarrage où l'état de mise en veille prolongée n'est pas conservé), cela peut être dû au fait que les données utilisateur contenaient le script suivant :

```
/usr/bin/enable-ec2-spot-hibernation
```

Supprimez ce script du champ Données utilisateur du modèle de lancement, puis demandez une nouvelle instance Spot.

Notez que même si l'instance n'a pas pu reprendre, si l'état de mise en veille prolongée n'est pas préservé, l'instance peut toujours être démarrée de la même manière qu'en partant de l'état `stopped`.

Redémarrer votre instance

Le redémarrage d'une instance est similaire à celui d'un système d'exploitation. Dans la plupart des cas, il suffit de quelques minutes pour redémarrer votre instance.

Lorsque vous redémarrez une instance, elle conserve les éléments suivants :

- Nom DNS public (IPv4)
- Adresse IPv4 privée

- Adresse IPv4 publique
- Adresse IPv6 (le cas échéant)
- Toutes les données présentes sur ses volumes de stockage d'instance

Le redémarrage d'une instance ne déclenche pas de nouvelle période de facturation (avec un minimum d'une minute), contrairement [à un arrêt et à un démarrage](#) d'une instance.

Il peut nous arriver de planifier le redémarrage d'une instance pour effectuer des tâches de maintenance, par exemple pour appliquer des mises à jour qui requièrent un redémarrage. Le cas échéant, aucune action n'est requise de votre part. Nous vous recommandons d'attendre simplement le redémarrage dans le créneau horaire prévu. Pour plus d'informations, consultez [Événements planifiés pour vos instances](#).

Nous vous recommandons d'utiliser la console Amazon EC2, un outil de ligne de commande ou l'API Amazon EC2 pour réamorcer votre instance au lieu d'exécuter la commande de réamorçage du système d'exploitation à partir de votre instance. Si vous utilisez la console Amazon EC2, un outil de ligne de commande ou l'API Amazon EC2 pour réamorcer votre instance, nous procédons à un redémarrage matériel si l'instance ne s'arrête pas correctement en quelques minutes. En revanche, si vous avez recours à AWS CloudTrail, l'utilisation d'Amazon EC2 pour redémarrer votre instance crée également un enregistrement d'API du moment où votre instance a été redémarrée.

instances Windows

Si Windows installe des mises à jour sur votre instance, nous vous conseillons de ne pas redémarrer ou arrêter votre instance en utilisant la console Amazon EC2 ou la ligne de commande tant que toutes les mises à jour ne sont pas installées. Si vous avez recours à la console Amazon EC2 ou à la ligne de commande pour redémarrer ou arrêter votre instance, votre instance peut faire l'objet d'un redémarrage matériel. Un redémarrage matériel pendant l'installation de mises à jour peut entraîner l'instabilité de votre instance.

Console

Pour redémarrer une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Instance state (État de l'instance), Reboot instance (Redémarrer l'instance).

Vous pouvez également sélectionner l'instance, puis choisir Actions, Manage instance state (Gérer l'état de l'instance). Dans l'écran qui s'ouvre, choisissez Reboot (Redémarrer), puis Change state (Modifier l'état).

4. Lorsque vous êtes invité à confirmer l'opération, sélectionnez Redémarrer.

L'instance reste dans l'état `running`.

Command line

Pour redémarrer une instance

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [reboot-instances](#) (AWS CLI)
- [Restart-EC2Instance](#) (AWS Tools for Windows PowerShell)

Pour exécuter une expérience d'injection de défauts contrôlés

Vous pouvez l'utiliser AWS Fault Injection Service pour tester la façon dont votre application répond lorsque votre instance est redémarrée. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Fault Injection Service](#).

Mettre fin aux instances Amazon EC2

Vous pouvez supprimer votre instance lorsque vous n'en avez plus besoin. Cette opération est appelée mise hors service (ou résiliation) de votre instance. Dès que l'état d'une instance passe à `shutting-down` ou `terminated`, l'instance ne vous est plus facturée.

Vous ne pouvez pas vous connecter à une instance mise hors service, ni la démarrer. Toutefois, vous pouvez lancer des instances supplémentaires à l'aide de la même AMI. Si vous préférez arrêter ou mettre en veille prolongée une instance, consultez [Arrêtez et démarrez les instances Amazon EC2](#) ou [Hibernez votre instance Amazon EC2](#). Pour plus d'informations, consultez [Différences entre redémarrage, arrêt, mise en veille prolongée et résiliation](#).

Table des matières

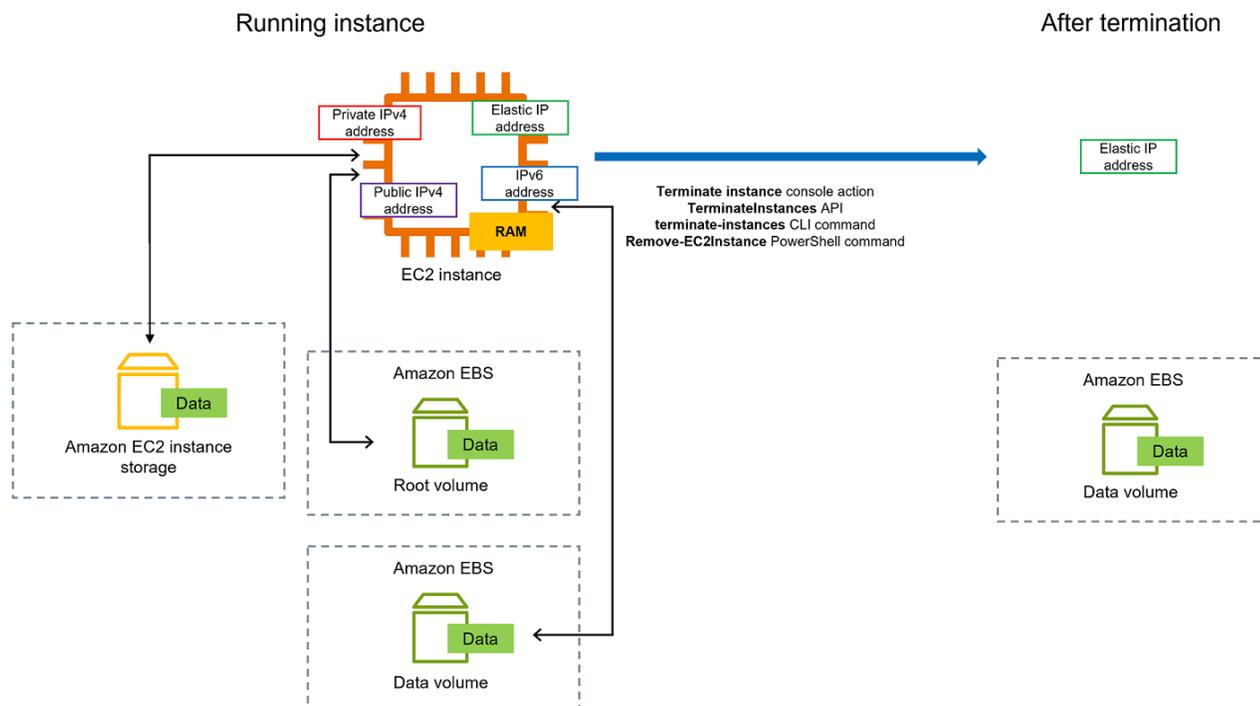
- [Comment fonctionne la résiliation d'une instance](#)

- [Résilier une instance](#)
- [Résoudre les problèmes de résiliation d'instance](#)
- [Activer la protection de la résiliation](#)
- [Modifier le comportement d'arrêt lancé de l'instance](#)
- [Conservation des données lors de la résiliation d'une instance](#)

Comment fonctionne la résiliation d'une instance

Lorsque vous mettez fin à une instance, les modifications sont enregistrées au niveau du système d'exploitation de l'instance, certaines ressources sont perdues et certaines ressources persistent.

Le schéma suivant montre ce qui est perdu et ce qui persiste lorsqu'une instance Amazon EC2 est résiliée. Lorsqu'une instance se termine, les données de tous les volumes de stockage d'instance et les données stockées dans la RAM de l'instance sont effacées. Toutes les adresses IP élastiques associées à l'instance sont détachées. Pour les volumes Amazon EBS et les données qu'ils contiennent, le résultat dépend du paramètre Supprimer en cas de résiliation du volume. Par défaut, le volume racine est supprimé et les volumes de données sont préservés.



Considérations

- Lorsqu'une instance est mise hors service, les données des volumes de stockage d'instances associées à cette instance sont supprimées.
- Par défaut, les volumes du périphérique racine Amazon EBS sont supprimés automatiquement lorsque l'instance est mise hors service. Toutefois, tout volume EBS supplémentaire attaché lors du lancement, ou tout volume EBS attaché à une instance existante, persiste même après la résiliation de l'instance. Pour plus d'informations, consultez [Conservation des données lors de la résiliation d'une instance](#).

Note

Tous les volumes qui ne sont pas supprimés lors de la résiliation de l'instance continueront à entraîner des frais.

- Pour éviter qu'une instance ne soit accidentellement interrompue par quelqu'un, [activez la protection contre la résiliation](#).
- Pour contrôler si une instance s'arrête ou se termine lorsque l'arrêt est initié à partir de l'instance, modifiez le [comportement d'arrêt initié par l'instance](#).
- Si vous exécutez un script de la résiliation d'une instance, il est possible que cette dernière soit résiliée de façon anormale dans la mesure où nous ne pouvons pas garantir le bon fonctionnement des scripts d'arrêt. Amazon EC2 tente de résilier une instance proprement et d'exécuter les scripts d'arrêt du système. Toutefois, certains événements (par exemple, une panne matérielle) peuvent empêcher l'exécution de ces scripts d'arrêt du système.

Ce qui se passe lorsque vous résiliez une instance

Modifications enregistrées au niveau du système d'exploitation

- La demande d'API envoie un événement d'appui sur un bouton à l'invité.
- Divers services système sont arrêtés à la suite de l'événement d'appui sur le bouton. L'arrêt progressif du système est assuré par systemd (Linux) ou le processus système (Windows). L'arrêt normal est déclenché par l'événement d'appui sur un bouton d'arrêt ACPI à partir de l'hyperviseur.
- L'arrêt ACPI est lancé.
- L'instance s'arrêtera une fois le processus d'arrêt progressif terminé. L'heure d'arrêt du système d'exploitation n'est pas configurable. L'instance reste visible dans la console pendant une courte période, puis l'entrée est automatiquement supprimée.

Ressources perdues

- Les données stockées sur un volume de stockage d'instances.
- Les données stockées sur les volumes de l'appareil racine Amazon EBS si l'attribut `DeleteOnTermination` est défini sur `true`.

Des ressources qui persistent

- Les données stockées sur des volumes Amazon EBS supplémentaires attachés lors du lancement ou après le lancement d'une instance.

Test de la réponse de l'application à la résiliation d'instance

Vous pouvez l'utiliser AWS Fault Injection Service pour tester la façon dont votre application réagit lorsque votre instance est arrêtée. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Fault Injection Service](#).

Résilier une instance

Vous pouvez mettre fin à une instance à tout moment.

Console

Pour résilier une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, choisissez État de l'instance, Résilier l'instance.
4. Choisissez Résilier lorsque vous êtes invité à confirmer.
5. Une fois que vous avez mis fin à une instance, elle reste visible pendant un court instant, avec un état `terminated`.

Si la résiliation échoue ou si une instance interrompue est visible pendant plus de quelques heures, consultez [Instance terminée toujours affichée](#).

Command line

Pour résilier une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [terminate-instances](#) (AWS CLI)
- [Remove-EC2Instance](#) (AWS Tools for Windows PowerShell)

Résoudre les problèmes de résiliation d'instance

Le demandeur doit être autorisé à appeler `ec2:TerminateInstances`. Pour plus d'informations, consultez la section [Exemples de politiques pour travailler avec les instances](#).

Si vous arrêtez votre instance et qu'une autre instance démarre, vous avez probablement configuré la mise à l'échelle automatique via une fonctionnalité comme flotte EC2 ou Amazon EC2 Auto Scaling. Pour plus d'informations, consultez [instances lancées ou terminées automatiquement](#).

Vous ne pouvez pas mettre fin à une instance si la protection contre la résiliation est activée. Pour plus d'informations, consultez la section [Protection contre le licenciement](#).

Si votre instance garde l'état `shutting-down` pendant plus longtemps que d'habitude, elle finit par être nettoyée (mise hors service) par les processus automatisés du service Amazon EC2. Pour plus d'informations, consultez [Mise à fin d'instance retardée](#).

Activer la protection de la résiliation

Pour éviter que votre instance ne soit résiliée accidentellement, vous pouvez activer la protection contre la résiliation pour l'instance. L'attribut `DisableApiTermination` contrôle si l'instance peut être interrompue à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de l'API. Par défaut, la protection contre la résiliation est désactivée pour votre instance, ce qui signifie que celle-ci peut être résiliée à l'aide de l'API AWS Management Console AWS CLI, ou. Vous pouvez définir la valeur de cet attribut lorsque vous lancez l'instance, pendant l'exécution de l'instance ou une fois l'instance arrêtée (pour les instances basées sur Amazon EBS).

L'attribut `DisableApiTermination` ne vous empêche pas de résilier une instance en déclenchant l'arrêt à partir de l'instance (à l'aide d'une commande du système d'exploitation pour l'arrêt système) lorsque l'attribut `InstanceInitiatedShutdownBehavior` est défini. Pour plus d'informations, consultez [Modifier le comportement d'arrêt lancé de l'instance](#).

Considérations

- L'activation de la protection contre la résiliation n' AWS empêche pas de mettre fin à l'instance lorsqu'un [événement planifié est prévu](#) pour mettre fin à l'instance.
- L'activation de la protection contre la résiliation n'empêche pas Amazon EC2 Auto Scaling de résilier une instance lorsque celle-ci est défectueuse ou pendant des événements de mise à l'échelle horizontale. Vous pouvez contrôler si un groupe Auto Scaling peut résilier une instance en particulier lors de la mise à l'échelle en utilisant la [protection contre la mise à l'échelle horizontale de l'instance](#). Vous pouvez contrôler si un groupe Auto Scaling peut résilier des instances défectueuses en [suspendant le processus de mise à l'échelle ReplaceUnhealthy](#).
- Vous ne pouvez pas activer la protection de la résiliation pour les instances Spot.

Pour activer la protection contre la résiliation d'une instance lors du lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le tableau de bord, sélectionnez Lancer une instance et suivez les instructions de l'assistant.
3. Sur la page Configurer les détails de l'instance, activez la case à cocher Activer la protection de la résiliation.

Pour activer la protection contre la résiliation d'une instance en cours d'exécution ou arrêtée

1. Sélectionnez l'instance, puis Actions, Instance Settings (Paramètres de l'instance) et Change Termination Protections (Changer la protection de la résiliation).
2. Choisissez Yes, Enable (Oui, Activer).

Pour désactiver la protection contre la résiliation d'une instance en cours d'exécution ou arrêtée

1. Sélectionnez l'instance, puis Actions, Instance Settings (Paramètres de l'instance) et Change Termination Protections (Changer la protection de la résiliation).
2. Choisissez Oui, désactiver.

Pour activer ou désactiver la protection contre la résiliation à l'aide de la ligne de commande.

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

Mettez fin à plusieurs instances grâce à une protection contre la résiliation

Si vous mettez fin à plusieurs instances dans plusieurs zones de disponibilité dans la même demande et qu'une ou plusieurs des instances spécifiées sont activées pour la protection contre la résiliation, la demande échoue avec les résultats suivants :

- Les instances spécifiées qui se trouvent dans la même zone de disponibilité que l'instance protégée ne sont pas résiliées.
- Les instances spécifiées qui se trouvent dans des zones de disponibilité différentes, où aucune autre instance spécifiée n'est protégée, sont résiliées avec succès.

Exemple

Supposons que vous disposiez des quatre instances suivantes réparties dans deux zones de disponibilité.

Instance	Zone de disponibilité	Protection contre la résiliation
Instance 1	EN TANT QUE	Disabled
Instance 2		Disabled
Instance 3	AZ B	Enabled
Instance 4		Disabled

Si vous tentez de résilier toutes ces instances dans la même demande, la demande signale un échec avec les résultats suivants :

- Les instances 1 et 2 sont mises hors service avec succès car aucune des deux instances n'est activée pour la protection contre les mises hors service.
- L'instance 3 et l'instance 4 ne parviennent pas à se terminer car l'instance 3 est activée pour la protection contre la résiliation.

Modifier le comportement d'arrêt lancé de l'instance

Par défaut, lorsque vous déclenchez un arrêt à partir d'une instance basée sur Amazon EBS (à l'aide d'une commande telle que `shutdown` ou `poweroff`), l'instance s'arrête. Vous pouvez modifier ce comportement pour que l'instance soit résiliée à la place en modifiant l'attribut `InstanceInitiatedShutdownBehavior` de l'instance. Vous pouvez modifier cet attribut tandis que l'instance est en cours d'exécution ou arrêtée.

La commande `halt` ne déclenche pas un arrêt. Si elle est utilisée, l'instance n'est pas résiliée. Au lieu de cela, elle place l'UC à l'état HLT et l'instance continue de s'exécuter.

Note

L'attribut `InstanceInitiatedShutdownBehavior` n'est applicable que si vous procédez à l'arrêt du système d'exploitation ou de l'instance elle-même. Cela ne s'applique pas lorsque vous arrêtez une instance à l'aide de l'API `StopInstances` ou de la console Amazon EC2.

Vous pouvez modifier l'attribut `InstanceInitiatedShutdownBehavior` à l'aide de la console Amazon EC2 ou de la ligne de commande.

Console

Pour modifier le comportement d'arrêt lancé de l'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Choisissez Actions, Paramètres d'instance, Modifier le comportement d'arrêt.

Comportement d'arrêt affiche le comportement actuel.

5. Pour modifier le comportement, pour Comportement d'arrêt, choisissez Arrêter ou Résilier.
6. Choisissez Enregistrer.

Command line

Pour modifier le comportement d'arrêt lancé de l'instance

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

Conservation des données lors de la résiliation d'une instance

Selon votre cas d'utilisation, vous souhaitez peut-être conserver les données sur votre volume de stockage d'instances ou sur le volume Amazon EBS lorsque l'instance Amazon EC2 est résiliée. Les données sur un volume de stockage d'instances ne persistent pas lorsqu'une instance est résiliée. Si vous devez conserver les données stockées sur un volume de stockage d'instances au-delà de la durée de vie de l'instance, vous devez copier manuellement ces données vers un stockage plus persistant, tel qu'un volume Amazon EBS, un compartiment Amazon S3 ou un système de fichiers Amazon EFS. Pour plus d'informations, consultez [Options de stockage pour vos instances Amazon EC2](#).

En ce qui concerne les données sur les volumes Amazon EBS, Amazon EC2 utilise la valeur de l'attribut `DeleteOnTermination` pour chaque volume Amazon EBS attaché afin de déterminer s'il faut conserver ou supprimer le volume.

La valeur par défaut de l'attribut `DeleteOnTermination` diffère selon que le volume est le volume racine de l'instance ou un volume non racine attaché à l'instance.

Volume racine

Par défaut, lorsque vous lancez une instance, l'attribut `DeleteOnTermination` du volume racine de l'instance est défini sur `true`. Par conséquent, l'action par défaut consiste à supprimer le volume racine de l'instance lorsque celle-ci est résiliée.

Volume non racine

Par défaut, lorsque vous attachez un volume EBS non root à une instance, son attribut `DeleteOnTermination` est défini sur `false`. L'action par défaut consiste donc à conserver ces volumes.

Note

Une fois l'instance mise hors service, vous pouvez prendre un instantané du volume conservé ou attacher celui-ci à une autre instance. Vous devez supprimer un volume pour éviter de générer des frais supplémentaires.

L'attribut `DeleteOnTermination` peut être défini par le créateur d'une AMI ou par la personne qui lance une instance. Lorsque l'attribut est modifié par le créateur d'une AMI ou par la personne qui lance une instance, le nouveau paramètre remplace le paramètre par défaut d'origine de l'AMI. Nous vous recommandons de vérifier le paramètre par défaut de l'attribut `DeleteOnTermination` après avoir lancé une instance avec une AMI.

Pour vérifier si un volume Amazon EBS sera supprimé lors de la résiliation de l'instance, consultez les détails du volume dans le volet des détails de l'instance. Dans l'onglet **Storage (Stockage)**, sous **Block devices (périphérique de stockage en mode bloc)**, faites défiler vers la droite pour afficher le paramètre **Delete on termination (supprimer à la date de résiliation)** pour le volume.

- Si la réponse est **Oui**, le volume sera supprimé lors de la résiliation de l'instance.
- Si la réponse est **Non**, le volume ne sera pas supprimé lors de la résiliation de l'instance. Tous les volumes qui ne sont pas supprimés lors de la résiliation de l'instance continueront à entraîner des frais.

Modifiez le volume racine pour qu'il persiste au lancement

À l'aide de la console, vous pouvez modifier l'attribut `DeleteOnTermination` lorsque vous lancez une instance. Pour modifier cet attribut lorsqu'il est associé à une instance en cours d'exécution, vous devez utiliser la ligne de commande.

Utilisez l'une des méthodes suivantes pour modifier le volume racine afin qu'il persiste lors du lancement.

Console

Pour modifier le volume racine d'une instance afin de le conserver lors du lancement à l'aide de la console

1. Suivez la procédure pour [lancer une instance](#), mais ne la lancez qu'après avoir effectué les étapes suivantes pour modifier le volume racine afin qu'il persiste.

2. Sous Stockage (volumes), développez les informations sous le volume racine.
3. Pour Supprimer à la résiliation, choisissez Oui.
4. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Command line

Modification du volume racine d'une instance pour qu'il persiste lors du lancement à l'aide de la ligne de commande

Lorsque vous lancez une instance basée sur EBS, vous pouvez utiliser l'une des commandes suivantes afin de modifier le volume du périphérique racine à conserver. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (AWS Tools for Windows PowerShell)

Dans les mappages de périphérique de stockage en mode bloc pour les volumes que vous voulez conserver, incluez `--DeleteOnTermination`, et spécifiez `false`.

Par exemple, pour conserver un volume, ajoutez l'option suivante à votre commande `run-instances` :

```
--block-device-mappings file://mapping.json
```

Dans `mapping.json`, indiquez le nom du périphérique, par exemple `/dev/sda1` ou `/dev/xvda`, et pour `--DeleteOnTermination`, indiquez `false`.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Modifier le volume racine d'une instance en cours d'exécution pour qu'il persiste

Vous pouvez utiliser l'une des commandes suivantes pour modifier le volume du périphérique racine d'une instance basée sur EBS en cours d'exécution afin de le conserver. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

Par exemple, utilisez la commande suivante :

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

Dans `mapping.json`, indiquez le nom du périphérique, par exemple `/dev/sda1` ou `/dev/xvda`, et pour `--DeleteOnTermination`, indiquez `false`.

```
[  
  {  
    "DeviceName": "device_name",  
    "Ebs": {  
      "DeleteOnTermination": false  
    }  
  }  
]
```

Mise hors service d'instance

La mise hors service d'une instance est planifiée lorsqu'une défaillance irréparable du matériel sous-jacent hébergeant l'instance est AWS détectée. Le périphérique racine de l'instance détermine le comportement de la mise hors service de l'instance :

- Si le périphérique racine de votre instance est un volume Amazon EBS, l'instance est arrêtée et vous pouvez la redémarrer à tout moment. Le démarrage de l'instance arrêtée la migre vers un nouveau matériel.
- Si le périphérique racine de votre instance est un volume de stockage d'instance, l'instance est résiliée et ne peut pas être réutilisée.

Pour plus d'informations sur les types d'événements d'instance, consultez [Événements planifiés pour vos instances](#).

Sommaire

- [Identifier des instances prévues pour une mise hors service](#)
- [Mesures à prendre sur les instances basées sur EBS dont la mise hors service est prévue](#)
- [Mesures à prendre pour les instances sauvegardées dans le stockage d'instances dont la mise hors service est prévue](#)

Identifier des instances prévues pour une mise hors service

Si votre instance est planifiée pour une mise hors service, vous recevez un courrier électronique préalable à l'événement avec l'ID d'instance et la date de mise hors service. Vous pouvez également rechercher les instances planifiées pour une mise hors service à l'aide de la console Amazon EC2 ou de la ligne de commande.

Important

Si une instance est programmée pour une mise hors service, nous vous recommandons de prendre des mesures dès que possible car elle peut être inaccessible. (La notification par e-mail que vous recevez indique ce qui suit : « En raison de cette dégradation, votre instance pourrait déjà être inaccessible. ») Pour plus d'informations sur les mesures recommandées, consultez [Check if your instance is reachable](#).

Comment identifier des instances prévues pour une mise hors service

- [Notification par e-mail](#)
- [Identification par la console](#)

Notification par e-mail

Si votre instance est planifiée pour une mise hors service, vous recevez un courrier électronique préalable à l'événement avec l'ID d'instance et la date de mise hors service.

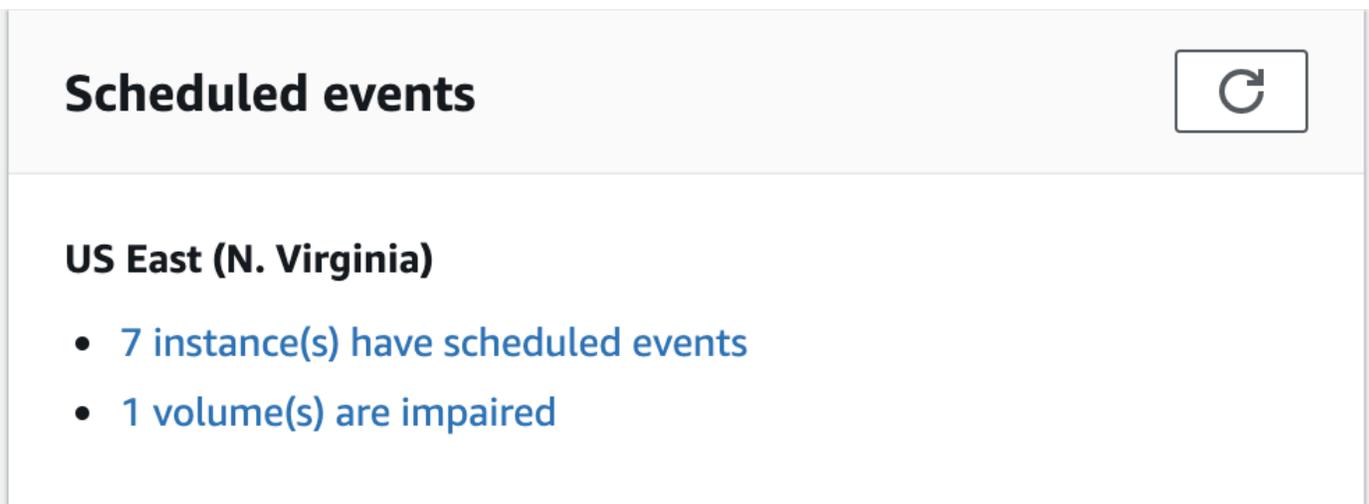
L'e-mail est envoyé au titulaire principal du compte et au contact des opérations. Pour plus d'informations, voir [Ajout, modification ou suppression de contacts alternatifs](#) dans le Guide de l'utilisateur AWS Billing .

Identification par la console

Si vous utilisez un compte de messagerie que vous ne consultez pas régulièrement en rapport avec les notifications de mise hors service d'instances, vous pouvez utiliser la console Amazon EC2 ou la ligne de commande pour déterminer si l'une de vos instances est planifiée pour la mise hors service.

Pour identifier les instances planifiées pour une mise hors service à l'aide de la console

1. Ouvrez la console Amazon EC2.
2. Dans le panneau de navigation, choisissez Tableau de bord du EC2. Sous Événements planifiés, vous pouvez voir les événements associés à vos instances et volumes Amazon EC2, organisés par région.



3. Si vous avez une instance avec un événement planifié affiché, sélectionnez le lien sous le nom de la région pour accéder à la page Événements.
4. La page Events répertorie toutes les ressources qui ont des événements associés. Pour afficher les instances planifiées pour une mise hors service, sélectionnez Instance resources dans la première liste de filtres, puis Instance stop or retirement dans la deuxième liste de filtres.
5. Si les résultats du filtre affichent une instance planifiée pour une mise hors service, sélectionnez-la et notez les date et heure dans le champ Start time du volet des détails. Il s'agit de la date de mise hors service de votre instance.

Pour identifier les instances planifiées pour une mise hors service à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [describe-instance-status](#) (AWS CLI)
- [Get-EC2InstanceStatus](#) (AWS Tools for Windows PowerShell)

Mesures à prendre sur les instances basées sur EBS dont la mise hors service est prévue

Pour conserver les données de votre instance mise hors service, vous pouvez effectuer l'une des actions suivantes. Il est important que vous preniez cette action avant la date de mise hors service de l'instance, afin de prévenir tout arrêt et perte de données imprévus.

Pour les instances Linux, si vous ne savez pas si votre instance est soutenue par EBS ou par un magasin d'instances, consultez [Déterminez le type de périphérique racine de votre instance Linux](#).

Vérifier si votre instance est accessible

Lorsque vous êtes averti que votre instance est programmée pour une mise hors service, nous vous recommandons de prendre les mesures suivantes dès que possible :

- Vérifiez si votre instance est accessible en vous [connectant](#) ou en envoyant une demande ping à celle-ci.
- Si votre instance est accessible, vous devez prévoir de l'arrêter/la démarrer à un moment approprié avant la date de mise hors service prévue, lorsque l'impact est minime. Pour plus d'informations sur l'arrêt et le redémarrage de votre instance, et sur ce que vous devez escompter quand votre instance est arrêtée, comme les conséquences sur les adresses publiques, privées et IP Elastic associées à votre instance, consultez [Arrêtez et démarrez les instances Amazon EC2](#). Veuillez noter que les données sur les volumes de stockage d'instances sont perdues lorsque vous arrêtez et démarrez votre instance.
- Si votre instance est inaccessible, vous devez prendre des mesures immédiates et effectuer un [arrêt/démarrage](#) pour la récupérer.
- Sinon, si vous souhaitez [mettre fin](#) à votre instance, prévoyez de le faire dès que possible, afin de cesser d'engager des frais pour cette dernière.

Créer une sauvegarde de votre instance

Pour disposer d'une sauvegarde, créez une AMI basée sur EBS à partir de votre instance. Pour garantir l'intégrité des données, arrêtez l'instance avant de créer l'AMI. Vous pouvez attendre la date de mise hors service planifiée quand l'instance est arrêtée ou arrêtez l'instance vous-même

avant la date de mise hors service. Vous pouvez redémarrer l'instance à tout moment. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).

Lancement d'une instance de remplacement

Après avoir créé une AMI à partir de votre instance, vous pouvez utiliser l'AMI pour lancer une instance de remplacement. Dans la console Amazon EC2, sélectionnez votre nouvelle AMI, puis choisissez Actions, Launch (Lancer). Suivez l'assistant pour lancer l'instance. Pour plus d'informations sur chaque étape de l'assistant, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Mesures à prendre pour les instances sauvegardées dans le stockage d'instances dont la mise hors service est prévue

Pour conserver les données de votre instance mise hors service, vous pouvez effectuer l'une des actions suivantes. Il est important que vous preniez cette action avant la date de mise hors service de l'instance, afin de prévenir tout arrêt et perte de données imprévus.

Warning

Si votre instance basée sur le stockage d'instances dépasse sa date de mise hors service, elle est terminée et vous ne pouvez pas récupérer l'instance ou les données qui y étaient stockées. Quel que soit le périphérique racine de votre instance, les données des volumes de stockage d'instances sont perdues quand l'instance est mise hors service, même si les volumes sont attachés à une instance basée sur EBS.

Vérifiez si votre instance est accessible

Lorsque vous êtes averti que votre instance est programmée pour une mise hors service, nous vous recommandons de prendre les mesures suivantes dès que possible :

- Vérifiez si votre instance est accessible en vous [connectant](#) ou en envoyant une demande ping à celle-ci.
- Si votre instance est inaccessible, les chances de la récupérer sont vraiment très réduites. Pour plus d'informations, consultez [Résolution d'un problème d'instance inaccessible](#). AWS mettra fin à votre instance à la date de mise hors service prévue. Ainsi, dans le cas d'une instance inaccessible, vous pouvez immédiatement [mettre fin à](#) l'instance vous-même.

Lancement d'une instance de remplacement

Créez une AMI basée sur le stockage d'instances à partir de votre instance à l'aide des outils AMI, comme décrit dans [Créer une AMI Linux basée sur le stockage d'instance](#). Dans la console Amazon EC2, sélectionnez votre nouvelle AMI, puis choisissez Actions, Launch (Lancer). Suivez l'assistant pour lancer l'instance. Pour plus d'informations sur chaque étape de l'assistant, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Convertir votre instance en instance basée sur EBS

Transférez vos données vers un volume EBS, prenez un instantané du volume, puis créez une AMI à partir de l'instantané. Vous pouvez lancer une instance de remplacement à partir de votre nouvel AMI. Pour plus d'informations, consultez [Convertir une AMI basée sur un stockage d'instance en AMI basée sur des volumes Amazon EBS](#).

Résilience de l'instance

Important

Les informations suivantes s'appliquent à la configuration des fonctionnalités liées à la restauration sur des instances saines. Si vous rencontrez actuellement des difficultés pour accéder à votre instance, consultez la section [Dépannage des instances EC2](#).

S'il s'avère qu' AWS une instance n'est pas disponible en raison d'un problème matériel sous-jacent, vous pouvez configurer deux mécanismes pour garantir la résilience de l'instance afin de rétablir la disponibilité : la restauration automatique simplifiée et la restauration basée sur CloudWatch l'action Amazon. Ce processus est appelé restauration d'instance.

Au moins un mécanisme doit être configuré ou activé à l'avance avec les ressources prises en charge pour que le processus de restauration de l'instance ait lieu. Par défaut, la restauration automatique simplifiée est activée pour les instances prises en charge lors de leur lancement.

Rubriques

- [Présentation de la restauration d'instances](#)
- [Alternatives de restauration d'instance](#)
- [Configuration de la restauration basée sur l' CloudWatch action](#)
- [Configuration d'une restauration automatique simplifiée](#)

Présentation de la restauration d'instances

Voici des exemples de problèmes matériels sous-jacents susceptibles de nécessiter une restauration d'instance :

- Perte de connectivité réseau
- Perte d'alimentation système
- Problèmes logiciels sur un hôte physique
- Problèmes matériels sur un hôte physique ayant un impact sur l'accessibilité du réseau

Une instance récupérée est identique à l'instance d'origine, notamment :

- ID d'instance
- Adresses IP publiques, privées et élastiques
- Métadonnées de l'instance
- Groupe de placement
- Volumes EBS joints
- Zone de disponibilité

Une restauration d'instance réussie apparaîtra à l'instance comme un redémarrage imprévu. En d'autres termes, le contenu stocké dans la mémoire volatile sera perdu, les données du stockage d'instance seront effacées et le temps de fonctionnement du système d'exploitation recommencera à zéro.

Pour vous protéger contre la perte de données, nous vous recommandons de créer régulièrement des sauvegardes de données importantes. Pour plus d'informations sur les meilleures pratiques de sauvegarde et de restauration pour les instances Amazon EC2, consultez la section [Meilleures pratiques pour Amazon EC2](#).

Alternatives de restauration d'instance

Les alternatives suivantes à la restauration d'instance peuvent être envisagées lorsqu'elles répondent au cas d'utilisation de vos instances.

Groupes Auto Scaling

Vous pouvez utiliser les groupes Auto Scaling pour regrouper un ensemble d'instances à des fins de dimensionnement et de disponibilité. Si une instance d'un groupe Auto Scaling devient indisponible, elle sera automatiquement remplacée (et non récupérée) par le groupe Auto Scaling. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon EC2 Auto Scaling ?](#) dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Amazon EBS Multi-Attach

Vous pouvez configurer Amazon EBS Multi-Attach pour vos instances afin de permettre à plusieurs instances d'être connectées au même volume EBS. Combiné à un logiciel approprié, cela permet d'activer le clustering à haute disponibilité. Pour un exemple de configuration avec des instances Linux, voir [Stockage en cluster simplifié : GFS2 sur les volumes compatibles avec Amazon EBS Multi-Attach](#) sur le blog de stockage. AWS

Configuration de la restauration basée sur l' CloudWatch action

Important

- Les informations suivantes s'appliquent à la configuration des fonctionnalités liées à la restauration sur des instances saines. Si vous rencontrez actuellement des difficultés pour accéder à votre instance, consultez la section [Dépannage des instances EC2](#).
- Pour que votre charge de travail fonctionne correctement après une restauration d'instance réussie, celle-ci doit démarrer et accepter le trafic sans intervention manuelle.

Vous pouvez configurer la restauration basée sur CloudWatch l'action Amazon pour ajouter des actions de restauration aux CloudWatch alarmes Amazon. CloudWatch la restauration basée sur l'action fonctionne avec la `StatusCheckFailed_System` métrique. CloudWatch la restauration basée sur les actions fournit une granularité du temps de réponse et des notifications Amazon Simple Notification Service (Amazon SNS) concernant les actions de to-the-minute restauration et les résultats. Ces options de configuration permettent des tentatives de restauration plus rapides grâce à un contrôle plus précis de la réponse à l'échec de la vérification de l'état du système, par rapport à une restauration automatique simplifiée. Pour plus d'informations sur les CloudWatch options disponibles, consultez la section [Contrôles de statut de vos instances](#).

La restauration basée sur CloudWatch l'action d'Amazon ne fonctionne pas lors d'événements de service dans le AWS Health Dashboard. Pour plus d'informations, consultez [the section called "Résolution des défaillances de restauration basées sur l' CloudWatchaction"](#).

Rubriques

- [Exigences et limites de la restauration basée sur CloudWatch l'action](#)
- [Configuration de la restauration basée sur l' CloudWatchaction](#)
- [Résolution des défaillances de restauration basées sur l' CloudWatchaction](#)

Exigences et limites de la restauration basée sur CloudWatch l'action

CloudWatch la restauration basée sur l'action peut tenter de récupérer une instance si elle :

- Est dans l'`running`État. Pour plus d'informations, consultez [the section called "Cycle de vie d'une instance"](#).
- Utilisations de `default` (à la demande) ou location d'`dedicatedinstance`. Pour plus d'informations, consultez [the section called "Options d'achat d'instance"](#).
- Il s'agit d'un type d'instance pour lequel Amazon EC2 dispose de capacités disponibles. Dans certaines situations, telles que des pannes importantes, la capacité disponible sera insuffisante et certaines tentatives de restauration risquent d'échouer.
- N'utilise pas la location d'`dedicatedinstance`. Pour les hôtes dédiés Amazon EC2, vous pouvez utiliser [récupération automatique de l'hôte dédié](#) pour récupérer automatiquement les instances défectueuses.
- N'utilise pas d'adaptateur Elastic Fabric.
- N'est pas membre d'un groupe Auto Scaling.
- Ne fait actuellement l'objet d'aucun événement de maintenance planifié.
- Utilise l'un des types d'instance suivants :
 - Usage général : A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
 - Optimisé pour le calcul : C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-Flex
 - Mémoire optimisée : R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | u-3tb1 | u-6tb1 | u-12tb1 | u-24tb1 | u-24tb1 | u7i-12tb | u7in-16tb | U7 en 24 TB | U7 en 32 TB | X1 | X1e | X2ieZN

- Calcul accéléré : G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
- Calcul haute performance : hPC6a | hPC7a | hPC7g
- Instances métalliques : n'importe lequel des types ci-dessus avec la taille de l'instance métallique.
- Possède des volumes de stockage d'instance et utilise l'un des types d'instance suivants : M3 | C3 | R3 | X1 | X1e | X2idn | X2iEDN

Warning

- Les données relatives aux volumes de stockage de l'instance seront perdues si l'instance est arrêtée. Pour plus d'informations sur l'arrêt d'une instance, consultez [the section called “Arrêt et démarrage de l'instance”](#).
- En cas d'échec de la vérification de l'état du système, les données mappées du périphérique de stockage et de bloc de l'instance peuvent être perdues. Pour ces types d'instances, vous pouvez envisager d'utiliser [the section called “Activer la protection de la résilience”](#).

Nous vous recommandons de créer régulièrement des sauvegardes de données importantes. Pour plus d'informations sur les meilleures pratiques de sauvegarde et de restauration pour Amazon EC2, consultez la section [Meilleures pratiques pour Amazon EC2](#).

Vous pouvez également utiliser le AWS Management Console ou le AWS CLI pour afficher les types d'instances qui prennent en charge la restauration basée sur CloudWatch l'action.

Console

Pour voir les types d'instances qui prennent en charge la restauration basée sur CloudWatch l'action d'Amazon

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, choisissez Instance Types (Types d'instance).
3. Dans la barre de filtre, saisissez Auto Recovery support: true (Prise en charge de la restauration automatique : vrai). Sinon, lorsque vous saisissez les caractères et que le nom du filtre apparaît, vous pouvez le sélectionner.

Le tableau des types d'instances affiche tous les types d'instances qui prennent en charge la restauration basée sur CloudWatch l'action Amazon.

AWS CLI

Pour voir les types d'instances qui prennent en charge la restauration basée sur CloudWatch l'action d'Amazon

Utilisez la commande [describe-instance-types](#).

```
aws ec2 describe-instance-types --filters Name=auto-recovery-supported,Values=true
--query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Configuration de la restauration basée sur l' CloudWatchaction

CloudWatch la restauration basée sur l'action fonctionne avec la `StatusCheckFailed_System` métrique. CloudWatch la restauration basée sur l'action est configurée via la CloudWatch console. Pour configurer la restauration basée sur CloudWatch l'action, consultez la section [Ajouter des actions de restauration aux CloudWatch alarmes](#) dans le guide de CloudWatch l'utilisateur Amazon.

Résolution des défaillances de restauration basées sur l' CloudWatchaction

Les problèmes suivants peuvent entraîner l'échec de la restauration de votre instance avec une restauration basée sur l' CloudWatch action :

- CloudWatch la restauration basée sur l'action ne fonctionne pas lors d'événements de service dans le AWS Health Dashboard. Il se peut que vous ne receviez pas de notifications d'échec de récupération pour de tels événements. Pour obtenir les dernières informations sur la disponibilité du service, consultez la page État [de santé du service](#).
- Capacité temporaire, insuffisante du matériel de remplacement.
- L'instance a atteint l'indemnité journalière maximale pour les tentatives de rétablissement. Votre instance pourrait ensuite être retirée si la récupération automatique échoue et si une dégradation matérielle est la cause première de l'échec du contrôle de statut du système d'origine.

Si l'échec de la vérification de l'état du système de l'instance persiste malgré plusieurs tentatives de restauration, consultez [Résoudre les problèmes des instances dont les vérifications d'état ont échoué](#) pour obtenir des instructions supplémentaires.

Configuration d'une restauration automatique simplifiée

Important

- Les informations suivantes s'appliquent à la configuration des fonctionnalités liées à la restauration sur des instances saines. Si vous rencontrez actuellement des difficultés pour accéder à votre instance, consultez la section [Dépannage des instances EC2](#).
- Pour que votre charge de travail fonctionne correctement après une restauration d'instance réussie, celle-ci doit démarrer et accepter le trafic sans intervention manuelle.

Par défaut, la restauration automatique simplifiée surveille toutes les instances en cours d'exécution prises en charge. En cas d'échec de la vérification de l'état du système, des tentatives de restauration automatique simplifiées visent à rétablir l'état sain de l'instance. La restauration automatique simplifiée ne fonctionne pas lors d'événements de service dans le AWS Health Dashboard. Pour plus d'informations, consultez [the section called "Résolution des défaillances de restauration automatique simplifiées"](#).

Lorsqu'un événement de restauration automatique simplifié se produit, vous recevez un AWS Health Dashboard événement. Pour configurer les notifications relatives à ces événements, reportez-vous à la section [Getting Started with Notifications des utilisateurs AWS](#) du guide de Notifications des utilisateurs AWS l'utilisateur. Vous pouvez également utiliser EventBridge les règles Amazon pour surveiller les événements de restauration automatique simplifiés à l'aide des codes d'événement suivants :

- AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS – événements réussis
- AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE – événements échoués

Pour plus d'informations, consultez les [EventBridge règles d'Amazon](#).

Rubriques

- [Exigences et limites pour une restauration automatique simplifiée](#)
- [Configuration d'une restauration automatique simplifiée](#)
- [Résolution des défaillances de restauration automatique simplifiées](#)

Exigences et limites pour une restauration automatique simplifiée

La restauration automatique simplifiée tentera de récupérer une instance si elle :

- Est dans l'`running` État. Pour plus d'informations, consultez [the section called "Cycle de vie d'une instance"](#).
- Utilisations `default` (à la demande) ou location `dedicatedinstance`. Pour plus d'informations, consultez [the section called "Options d'achat d'instance"](#).
- Il s'agit d'un type d'instance pour lequel Amazon EC2 dispose de capacités disponibles. Dans certaines situations, telles que des pannes importantes, la capacité disponible sera insuffisante et certaines tentatives de restauration risquent d'échouer.
- N'utilise pas la location `dedicatedinstance`. Pour les hôtes dédiés Amazon EC2, vous pouvez utiliser [récupération automatique de l'hôte dédié](#) pour récupérer automatiquement les instances défectueuses.
- N'utilise pas d'adaptateur Elastic Fabric.
- Il ne s'agit pas d'une taille `metalinstance`.
- N'est pas membre d'un groupe Auto Scaling.
- Ne fait actuellement l'objet d'aucun événement de maintenance planifié.
- Ne possède pas de volumes de stockage d'instance.
- Utilise l'un des types d'instance suivants :
 - Usage général : A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
 - Optimisé pour le calcul : C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7i | C7i-Flex
 - Mémoire optimisée : R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | u-3tb1 | u-6tb1 | u-12tb1 | u-24tb1 | u-24tb1 | u7i-12tb | u7in-16tb | U7 en 24 TB | U7 en 32 TB | X1 | X1e | X2ieZN
 - Calcul accéléré : G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
 - Calcul haute performance : hPC6a | hPC7a | hPC7g

Warning

- Les données relatives aux volumes de stockage de l'instance seront perdues si l'instance est arrêtée. Pour plus d'informations sur l'arrêt d'une instance, consultez [the section called “Arrêt et démarrage de l'instance”](#).
- En cas d'échec de la vérification de l'état du système, les données mappées du périphérique de stockage et de bloc de l'instance peuvent être perdues. Pour ces types d'instances, vous pouvez envisager d'utiliser [the section called “Activer la protection de la résiliation”](#).

Nous vous recommandons de créer régulièrement des sauvegardes de données importantes. Pour plus d'informations sur les meilleures pratiques de sauvegarde et de restauration pour Amazon EC2, consultez la section [Meilleures pratiques pour Amazon EC2](#).

Configuration d'une restauration automatique simplifiée

La restauration automatique simplifiée est activée par défaut lorsque vous lancez une instance prise en charge. Vous pouvez définir le comportement de restauration automatique disabled pendant ou après le lancement de l'instance. La default configuration n'active pas la restauration automatique simplifiée pour un type d'instance non pris en charge.

Console

Pour désactiver la récupération automatique simplifiée lors du lancement de l'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances, puis Launch instance (Lancer une instance).
3. Dans la section Advanced details (Détails avancés), pour nstance auto-recovery (Récupération automatique de l'instance), sélectionnez Disabled (Désactivé).
4. Configurez les paramètres de lancement de l'instance restants selon les besoins, puis lancez l'instance.

Désactivation de la récupération automatique simplifiée d'une instance en cours d'exécution ou arrêtée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance, puis choisissez Actions, Instance Settings (Paramètres de l'instance), Change auto-recovery Behavior (Changer le comportement de restauration automatique).
4. Choisissez Off (Désactiver), puis Save (Enregistrer).

Pour définir le comportement de récupération automatique sur **default** pour une instance en cours d'exécution ou arrêtée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance, puis choisissez Actions, Instance Settings (Paramètres de l'instance), Change auto-recovery Behavior (Changer le comportement de restauration automatique).
4. Choisissez Par défaut (Activé), puis Enregistrer.

AWS CLI

Désactivation de la récupération automatique simplifiée au lancement

Utilisez la commande [run-instances](#).

```
aws ec2 run-instances \  
--image-id ami-1a2b3c4d \  
--instance-type t2.micro \  
--key-name MyKeyPair \  
--maintenance-options AutoRecovery=Disabled \  
[...]
```

Désactivation de la récupération automatique simplifiée d'une instance en cours d'exécution ou arrêtée

Utilisez la commande [modify-instance-maintenance-options](#).

```
aws ec2 modify-instance-maintenance-options \  
--instance-id i-0abcdef1234567890 \  
[...]
```

```
--auto-recovery disabled
```

Pour définir le comportement de récupération automatique sur **default** pour une instance en cours d'exécution ou arrêtée

Utilisez la commande [modify-instance-maintenance-options](#).

```
aws ec2 modify-instance-maintenance-options \  
--instance-id i-0abcdef1234567890 \  
--auto-recovery default
```

Résolution des défaillances de restauration automatique simplifiées

Les problèmes suivants peuvent entraîner l'échec de la restauration de votre instance avec restauration automatique simplifiée :

- La restauration automatique simplifiée ne fonctionne pas lors d'événements de service dans le AWS Health Dashboard. Il se peut que vous ne receviez pas de notifications d'échec de récupération pour de tels événements. Pour obtenir les dernières informations sur la disponibilité du service, consultez la page État [de santé du service](#).
- Capacité temporaire, insuffisante du matériel de remplacement.
- L'instance a atteint l'indemnité journalière maximale pour les tentatives de rétablissement. Votre instance pourrait ensuite être retirée si la récupération automatique échoue et si une dégradation matérielle est la cause première de l'échec du contrôle de statut du système d'origine.

Si l'échec de la vérification de l'état du système de l'instance persiste malgré plusieurs tentatives de restauration, consultez [Résoudre les problèmes des instances dont les vérifications d'état ont échoué](#) pour obtenir des instructions supplémentaires.

Utiliser des métadonnées d'instance

Les métadonnées d'instance sont des données portant sur votre instance que vous pouvez utiliser pour configurer ou gérer l'instance en cours d'exécution. Les métadonnées d'instance sont divisées en [catégories](#), par exemple, nom d'hôte, événements et groupes de sécurité.

Vous pouvez également utiliser les métadonnées d'instance pour accéder aux données utilisateur que vous avez spécifiées au moment du lancement de votre instance. Par exemple, vous pouvez spécifier des paramètres pour la configuration de votre instance ou inclure un script simple. Vous

pouvez également créer des AMI génériques et utiliser les données utilisateur pour modifier les fichiers de configuration fournis au moment du lancement. Par exemple, si vous gérez des serveurs Web pour différentes petites entreprises, elles peuvent toutes utiliser la même AMI générique et récupérer leur contenu à partir d'un compartiment Amazon S3 que vous spécifiez dans les données utilisateur au lancement. Pour ajouter un nouveau client à n'importe quel moment, créez un compartiment pour le client, ajoutez son contenu, puis lancez votre AMI avec l'unique nom de compartiment fourni à votre code dans les données utilisateur. Si vous lancez plusieurs instances à l'aide du même `RunInstances` appel, les données utilisateur sont disponibles pour toutes les instances de cette réservation. Chaque instance faisant partie de la même réservation possède un `ami-launch-index` numéro unique, ce qui vous permet d'écrire du code qui contrôle ce que font les instances. Par exemple, le premier hôte peut s'écrire comme nœud d'origine dans un cluster. Pour un exemple détaillé de lancement d'AMI, consultez [Exemple Linux : valeur de l'index de lancement de l'AMI](#).

Les instances EC2 peuvent également comprendre des données dynamiques, par exemple un document d'identité d'instance qui est généré au lancement de l'instance. Pour plus d'informations, consultez [Catégories de données dynamiques](#).

Important

Bien que les métadonnées d'instance et les données utilisateur ne soient accessibles qu'au sein de l'instance elle-même, elles ne sont pas protégées par des méthodes d'authentification ou de chiffrement. Toute personne ayant un accès direct à l'instance, et potentiellement tout logiciel s'exécutant sur l'instance, peut afficher ses métadonnées. Vous ne devez donc pas stocker de données sensibles, telles que des mots de passe ou des clés de chiffrement à longue durée, ou des données utilisateur.

Table des matières

- [Utiliser IMDSv2](#)
- [Configurer les options de métadonnées d'instance](#)
- [Récupérer des métadonnées d'instance](#)
- [Utiliser les données utilisateur d'instance](#)
- [Récupérer des données dynamiques](#)
- [Catégories de métadonnées d'instance](#)
- [Exemple Linux : valeur de l'index de lancement de l'AMI](#)

- [Documents d'identité d'instance](#)
- [Rôles d'identité d'instance](#)

Utiliser IMDSv2

Vous pouvez accéder aux métadonnées d'instance à partir d'une instance en cours d'exécution en utilisant l'une des méthodes suivantes :

- Service des métadonnées d'instance Version 1 (IMDSv1) – méthode de demande/réponse
- Service des métadonnées d'instance Version 2 (IMDSv2) – méthode orientée session

Par défaut, vous pouvez utiliser IMDSv1 ou IMDSv2, ou les deux.

Vous pouvez configurer le service des métadonnées d'instance (IMDS) sur chaque instance afin que le code local ou les utilisateurs locaux doivent utiliser IMDSv2. Lorsque vous spécifiez que IMDSv2 doit être utilisé, IMDSv1 ne fonctionne plus. Pour plus d'informations sur la configuration de votre instance pour l'utilisation d'IMDSv2, veuillez consulter la rubrique [Configurer les options de métadonnées d'instance](#).

Les en-têtes PUT ou GET sont uniques à IMDSv2. Si ces en-têtes sont présents dans la requête, celle-ci est destinée à IMDSv2. Si aucun en-tête n'est présent, on suppose que la requête est destinée à IMDSv1.

Pour un examen approfondi d'IMDSv2, veuillez consulter le billet de blog [Add defense in depth against open firewalls, reverse proxies, and SSRF vulnerabilities with enhancements to the EC2 Instance Metadata Service](#).

Pour récupérer des métadonnées d'instance, consultez [Récupérer des métadonnées d'instance](#).

Rubriques

- [Fonctionnement de Service des métadonnées d'instance Version 2](#)
- [Passer à l'utilisation de Service des métadonnées d'instance Version 2](#)
- [Utilisation d'un kit SDK AWS pris en charge](#)

Fonctionnement de Service des métadonnées d'instance Version 2

IMDSv2 utilise des demandes orientées session. Lorsque vous utilisez des demandes orientées session, vous créez un jeton de session qui définit la durée de la session, qui doit être d'une seconde au minimum et de six heures au maximum. Durant la période spécifiée, vous pouvez utiliser le même jeton de session pour les demandes suivantes. Une fois la période spécifiée arrivée à expiration, vous devez créer un nouveau jeton de session à utiliser pour les futures demandes.

Note

Les exemples de cette section utilisent l'adresse IPv4 du service des métadonnées d'instance (IMDS) : 169.254.169.254. Si vous récupérez des métadonnées d'instance pour les instances EC2 sur l'adresse IPv6, assurez-vous d'activer et d'utiliser l'adresse IPv6 à la place : [fd00:ec2::254]. L'adresse IPv6 de l'IMDS est compatible avec les commandes IMDSv2. L'adresse IPv6 n'est accessible que sur [les instances créées sur le système AWS Nitro](#) et dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement).

Les exemples suivants utilisent un script shell et IMDSv2 pour récupérer les éléments de métadonnées de l'instance de niveau supérieur. Chaque exemple :

- Crée un jeton de session d'une durée de six heures (21 600 secondes) en utilisant la demande PUT
- Stocke l'en-tête du jeton de session dans une variable nommée TOKEN (instances Linux) ou token (instances Windows)
- Demande les éléments de métadonnées de haut niveau à l'aide du jeton

Exemple Linux

Vous pouvez exécuter deux commandes distinctes ou les combiner.

Commandes distinctes

Tout d'abord, générez un jeton à l'aide de la commande suivante.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" `
```

Utilisez ensuite le jeton pour générer des éléments de métadonnées de niveau supérieur à l'aide de la commande suivante.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Commandes combinées

Vous pouvez stocker le jeton et combiner les commandes. L'exemple suivant combine les deux commandes ci-dessus et stocke l'en-tête du jeton de session dans une variable nommée TOKEN.

Note

En cas d'erreur lors de la création du jeton, un message d'erreur remplace le jeton valide dans la variable et la commande ne fonctionne pas.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Une fois que vous avez créé un jeton, vous pouvez le réutiliser jusqu'à son expiration. Dans l'exemple de commande suivant, qui extrait l'ID de l'AMI utilisée pour lancer l'instance, le jeton stocké dans \$TOKEN dans l'exemple précédent est réutilisé.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-id
```

Exemple Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/
```

Une fois que vous avez créé un jeton, vous pouvez le réutiliser jusqu'à son expiration. Dans l'exemple de commande suivant, qui extrait l'ID de l'AMI utilisée pour lancer l'instance, le jeton stocké dans \$token dans l'exemple précédent est réutilisé.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
-Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Lorsque vous utilisez IMDSv2 pour demander les métadonnées d'une instance, la demande doit inclure les éléments suivants :

1. Utilisez une demande PUT pour lancer une session sur le service des métadonnées d'instance. La demande PUT renvoie un jeton qui doit être inclus dans les demandes GET suivantes envoyées au service des métadonnées d'instance. Le jeton est obligatoire pour accéder aux métadonnées à l'aide de IMDSv2.
2. Incluez le jeton dans toutes les demandes GET envoyées à l'IMDS. Lorsque l'utilisation de jeton est définie sur `required`, les demandes sans jeton valide ou contenant un jeton arrivé à expiration reçoivent un code d'erreur HTTP 401 - `Unauthorized`.
 - Le jeton est une clé propre à l'instance. Le jeton n'est pas valide sur les autres instances EC2 et sera rejeté si vous tentez de l'utiliser ailleurs que sur l'instance sur laquelle il a été généré.
 - La demande PUT doit inclure un en-tête spécifiant la durée `time-to-live (TTL)` du jeton, en secondes, jusqu'à six heures au maximum (21 600 secondes). Le jeton représente une session logique. La durée de vie (TTL) définit la durée de validité du jeton et, par conséquent, la durée de la session.
 - Une fois qu'un jeton est arrivé à expiration, pour pouvoir continuer à accéder aux métadonnées de l'instance, vous devez créer une nouvelle session en utilisant un autre PUT.
 - Vous pouvez choisir de réutiliser un jeton ou d'en créer un nouveau pour chaque demande. Pour un faible nombre de demandes, il peut être plus facile de générer et d'utiliser immédiatement un jeton chaque fois que vous avez besoin d'accéder à l'IMDS. Cependant, pour une plus grande productivité, vous pouvez spécifier une durée plus longue pour le jeton et le réutiliser plutôt que de devoir écrire une demande PUT chaque fois que vous avez besoin de demander des métadonnées d'instance. Il n'existe pas de limite pratique au nombre de jetons simultanés, chacun représentant sa propre session. IMDSv2 est toutefois soumis aux limites normales de connexion de l'IMDS. Pour plus d'informations, consultez [Limitation des demandes](#).

Les méthodes HTTP GET et HEAD sont autorisées dans les demandes de métadonnées d'instance IMDSv2. Les demandes PUT sont rejetées si elles contiennent un en-tête `X-Forwarded-For`.

Par défaut, la réponse aux demandes PUT possède une durée `time-to-live (hop limit)` de réponse de 1 au niveau du protocole IP. Si vous avez besoin d'une limite de sauts plus élevée, vous pouvez l'ajuster à l'aide de la commande [AWS CLI modify-instance-metadata-options](#). Par exemple, vous

pouvez avoir besoin d'une durée de vie plus élevée pour des raisons de compatibilité en amont avec les services de conteneur s'exécutant sur l'instance. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les instances existantes](#).

Passer à l'utilisation de Service des métadonnées d'instance Version 2

Lorsque vous effectuez la migration vers IMDSv2, nous vous recommandons d'utiliser les outils et le chemin de transition suivants.

Rubriques

- [Outils facilitant la migration vers IMDSv2](#)
- [Chemin recommandé pour demander l'accès à IMDSv2](#)

Outils facilitant la migration vers IMDSv2

Si votre logiciel utilise IMDSv1, utilisez les outils suivants pour faciliter sa reconfiguration vers IMDSv2.

AWS logiciel

Les dernières versions du AWS SDK AWS CLI et du kit de développement prennent en charge l'IMDSv2. Pour utiliser IMDSv2, veillez à ce que vos instances EC2 possèdent les dernières versions de la CLI et des kits SDK. Pour plus d'informations sur la mise à jour de la CLI, consultez [Installation, mise à jour et désinstallation d' AWS CLI](#) dans le Guide de l'utilisateur AWS Command Line Interface .

Tous les packages logiciels Amazon Linux 2 et Amazon Linux 2023 sont compatibles avec IMDSv2. Dans Amazon Linux 2023, IMDSv1 est désactivé par défaut.

Pour connaître les versions minimales du AWS SDK compatibles avec IMDSv2, consultez [Utilisation d'un kit SDK AWS pris en charge](#)

Analyseur de packages IMDS

L'analyseur de packages IMDS est un outil open source qui identifie et journalise les appels IMDSv1 depuis la phase de démarrage de votre instance. Cela peut aider à identifier le logiciel qui effectue des appels IMDSv1 sur les instances EC2, ce qui vous permet de déterminer exactement ce que vous devez mettre à jour pour que vos instances soient prêtes à utiliser IMDSv2 uniquement. Vous pouvez exécuter l'analyseur de packages IMDS à partir d'une ligne de

commande ou l'installer en tant que service. Pour plus d'informations, consultez la section [IMDS Packet Analyzer activé](#). [GitHub](#)

CloudWatch

IMDSv2 utilise des sessions basées sur un jeton, mais pas IMDSv1. La `MetadataNoToken` CloudWatch métrique suit le nombre d'appels au service de métadonnées d'instance (IMDS) qui utilisent IMDSv1. En suivant cette métrique jusqu'à zéro, vous pouvez déterminer si la totalité de votre logiciel a été mis à niveau vers IMDSv2 et le moment auquel cela se produit.

Après avoir désactivé IMDSv1, vous pouvez utiliser la `MetadataNoTokenRejected` CloudWatch métrique pour suivre le nombre de tentatives et de refus d'un appel IMDSv1. En suivant cette métrique, vous pouvez déterminer si votre logiciel doit être mis à jour pour utiliser IMDSv2.

Pour plus d'informations, consultez [Métriques des instances](#).

Mises à jour des API et des CLI EC2

Pour les nouvelles instances, vous pouvez utiliser l'[RunInstances](#) API pour lancer de nouvelles instances qui nécessitent l'utilisation d'IMDSv2. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les nouvelles instances](#).

Pour les instances existantes, vous pouvez utiliser l'[ModifyInstanceMetadataOptions](#) API pour exiger l'utilisation d'IMDSv2. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les instances existantes](#).

Pour exiger l'utilisation de IMDSv2 sur toutes les nouvelles instances lancées par des groupes Auto Scaling, ces derniers peuvent utiliser un modèle de lancement ou une configuration de lancement. Lorsque vous [créez un modèle de lancement](#) ou [une configuration de lancement](#), vous devez configurer les paramètres `MetadataOptions` pour exiger l'utilisation de IMDSv2. Le groupe Auto Scaling lance de nouvelles instances à l'aide du nouveau modèle de lancement ou de la nouvelle configuration de lancement, mais les instances existantes ne sont pas affectées. Pour les instances existantes d'un groupe Auto Scaling, vous pouvez utiliser l'[ModifyInstanceMetadataOptions](#) API pour exiger l'utilisation d'IMDSv2 sur les instances existantes, ou mettre fin aux instances et le groupe Auto Scaling lancera de nouvelles instances de remplacement avec les paramètres des options de métadonnées d'instance définis dans le nouveau modèle de lancement ou dans la nouvelle configuration de lancement.

Utilisation d'une AMI qui configure IMDSv2 par défaut

Lorsque vous lancez une instance, vous pouvez la configurer automatiquement pour utiliser IMDSv2 par défaut (le paramètre `HttpTokens` est défini sur `required`) en la lançant avec une AMI configurée avec le paramètre `ImdsSupport` défini sur `v2.0`. Vous pouvez définir le paramètre `ImdsSupport` sur `v2.0` lorsque vous enregistrez l'AMI à l'aide de la commande CLI [register-image](#), ou vous pouvez modifier une AMI existante à l'aide de la commande CLI [modify-image-attribute](#). Pour plus d'informations, consultez [Configurer l'AMI](#).

Politiques IAM et politiques de contrôle des services

Vous pouvez utiliser une stratégie IAM ou une politique de contrôle des AWS Organizations services (SCP) pour contrôler les utilisateurs comme suit :

- Impossible de lancer une instance à l'aide de l'[RunInstances](#) API à moins que l'instance ne soit configurée pour utiliser IMDSv2.
- Impossible de modifier une instance en cours d'exécution à l'aide de l'[ModifyInstanceMetadataOptions](#) API pour réactiver IMDSv1.

La politique IAM ou la politique de contrôle des services doit contenir les clés de condition IAM suivantes :

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Si un paramètre de l'appel d'API ou de CLI ne correspond pas à l'état spécifié dans la politique contenant la clé de condition, l'appel de l'API ou de la CLI échoue avec la réponse `UnauthorizedOperation`.

Vous pouvez en outre choisir une couche de protection supplémentaire afin d'imposer le passage de IMDSv1 à IMDSv2. Au niveau de la couche de gestion des accès, en ce qui concerne les API appelées via les informations d'identification du rôle EC2, vous pouvez utiliser une nouvelle clé de condition dans les politiques IAM ou les politiques de contrôle des AWS Organizations services (SCP). Si vous utilisez la clé de condition `ec2:RoleDelivery` avec la valeur `2.0` dans vos politiques IAM, les appels d'API effectués avec des informations d'identification de rôle EC2 obtenues à partir de IMDSv1 recevront une réponse `UnauthorizedOperation`. Vous pouvez aboutir au même résultat plus généralement avec cette condition requise par une SCP. Cela permet de s'assurer que les informations d'identification fournies via IMDSv1 ne peuvent pas être utilisées pour appeler des API, car tout appel d'API ne respectant pas la condition spécifiée recevra une erreur `UnauthorizedOperation`.

Par exemple les stratégies IAM, consultez [Utiliser des métadonnées d'instance](#). Pour plus d'informations sur les politiques de contrôle des services, consultez [Politiques de contrôle des services](#) dans le Guide de l'utilisateur AWS Organizations .

Chemin recommandé pour demander l'accès à IMDSv2

Nous vous recommandons, tout en utilisant les outils mentionnés précédemment, de suivre ce chemin pour la migration vers IMDSv2.

Étape 1 : Au départ

Mettez à jour les kit SDK, les CLI et vos logiciels utilisant des informations d'identification de rôle sur leurs instances EC2 vers des versions compatibles avec IMDSv2. Pour plus d'informations sur la mise à jour de la CLI, consultez [Mise à niveau vers la dernière version d' AWS CLI](#) dans le Guide de l'utilisateur AWS Command Line Interface .

Modifiez ensuite les logiciels accédant directement aux métadonnées de l'instance (en d'autres termes, n'utilisant pas un kit SDK) à l'aide des demandes IMDSv2. Vous pouvez utiliser l'[analyseur de packages IMDS](#) pour identifier le logiciel que vous devez modifier pour utiliser les requêtes IMDSv2.

Étape 2 : suivre la progression de votre transition

Suivez la progression de votre transition à l'aide de la CloudWatch métrique `MetadataNoToken`. Cette métrique indique le nombre d'appels IMDSv1 à l'IMDS sur vos instances. Pour plus d'informations, consultez [Métriques des instances](#).

Étape 3 : quand il n'y a aucune utilisation de IMDSv1

Lorsque la CloudWatch métrique `MetadataNoToken` enregistre une utilisation nulle d'IMDSv1, vos instances sont prêtes à passer entièrement à l'utilisation d'IMDSv2. A ce stade, voici ce que vous pouvez faire :

- Compte par défaut

Vous pouvez configurer IMDSv2 pour qu'il soit obligatoire comme compte par défaut. Lorsqu'une instance est lancée, la configuration de l'instance est automatiquement définie sur la valeur par défaut du compte.

Pour définir le compte par défaut, procédez comme suit :

- Console Amazon EC2 : sur le tableau de bord EC2, sous Attributs du compte, Protection et sécurité des données, pour les valeurs par défaut de l'IMDS, définissez le service de métadonnées de l'instance sur Activé et la version des métadonnées sur V2 uniquement (jeton requis). Pour plus d'informations, consultez [Définissez IMDSv2 comme valeur par défaut pour le compte](#).
- AWS CLI: utilisez la commande CLI [modify-instance-metadata-defaults](#) et spécifiez `et. --http-tokens required --http-put-response-hop-limit 2`
- Nouvelles instances

Lors du lancement d'une nouvelle instance, vous pouvez effectuer les opérations suivantes :

- Console Amazon EC2 : dans l'assistant de lancement d'instance, définissez Metadata accessible (Métadonnées accessibles) sur Enabled (Activé) et Metadata version (Version des métadonnées) sur V2 only (token required) (V2 uniquement [jeton obligatoire]). Pour plus d'informations, consultez [Configurer l'instance au lancement](#).
- AWS CLI: utilisez la commande [run-instances CLI](#) et spécifiez que IMDSv2 est requis.
- Instances existantes

Pour les instances existantes, vous pouvez exécuter les opérations suivantes :

- Console Amazon EC2 : sur la page Instances, sélectionnez votre instance, choisissez Actions, Paramètres de l'instance, Modifier les options des métadonnées d'instance et, pour IMDSv2, choisissez Requis. Pour plus d'informations, consultez [Exigence d'utilisation d'IMDSv2](#).
- AWS CLI : utilisez la commande CLI [modify-instance-metadata-options](#) pour spécifier que seul l'IMDSv2 doit être utilisé.

Vous pouvez modifier les options des métadonnées d'instance sur les instances en cours d'exécution, et vous n'avez pas besoin de redémarrer les instances après avoir modifié ces options.

Étape 4 : vérifiez que vos instances ont bien été migrées vers IMDSv2

Vous pouvez vérifier si des instances ne sont pas encore configurées pour l'utilisation d'IMDSv2. En d'autres termes, si IMDSv2 est toujours configuré comme `optional`. Si des instances sont toujours configurées sur `optional`, vous pouvez modifier les options des métadonnées d'instance pour rendre IMDSv2 `required` en répétant l'[étape 3](#) précédente.

Pour filtrer vos instances :

- Console Amazon EC2 : sur la page Instances, filtrez vos instances à l'aide du filtre IMDSv2 = facultatif. Pour plus d'informations sur le filtrage, veuillez consulter la rubrique [Filtrer des ressources à l'aide de la console](#). Vous pouvez également voir si IMDSv2 est requis ou facultatif pour chaque instance : dans la fenêtre Préférences, activez IMDSv2 pour ajouter la colonne IMDSv2 au tableau Instances.
- AWS CLI : utilisez la commande CLI [describe-instances](#) et filtrez par `metadata-options.http-tokens = optional`, comme suit :

```
aws ec2 describe-instances --filters "Name=metadata-options.http-tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --output text
```

Étape 5 : lorsque toutes vos instances ont été migrées sur IMDSv2

Les clés de condition `ec2:MetadataHttpTokensec2:MetadataHttpPutResponseHopLimit`, et `ec2:MetadataHttpEndpoint` IAM peuvent être utilisées pour contrôler l'utilisation des [ModifyInstanceMetadataOptions](#) API [RunInstances](#) et des CLI correspondantes. Si une stratégie est créée et qu'un paramètre de l'appel d'API ne correspond pas à l'état spécifié dans la stratégie à l'aide de la clé de condition, l'appel de l'API ou de l'interface de ligne commande échoue avec la réponse `UnauthorizedOperation`. Par exemple les stratégies IAM, consultez [Utiliser des métadonnées d'instance](#).

En outre, après avoir désactivé IMDSv1, vous pouvez utiliser la `MetadataNoTokenRejected` CloudWatch métrique pour suivre le nombre de fois qu'un appel IMDSv1 a été tenté et rejeté. Si, après avoir désactivé IMDSv1, vous avez un logiciel qui ne fonctionne pas correctement et que la `MetadataNoTokenRejected` métrique enregistre les appels IMDSv1, il est probable que ce logiciel doit être mis à jour pour utiliser IMDSv2.

Utilisation d'un kit SDK AWS pris en charge

Pour utiliser IMDSv2, vos instances EC2 doivent utiliser une version du AWS SDK qui prend en charge l'utilisation d'IMDSv2. Les dernières versions de tous les AWS SDK prennent en charge l'utilisation d'IMDSv2.

Important

Nous vous recommandons de vous tenir au courant des versions du kit SDK afin de rester à jour avec les dernières fonctionnalités, mises à jour de sécurité et dépendances sous-

jaçentes. L'utilisation continue d'une version du kit SDK non prise en charge n'est pas recommandée et est effectuée à votre discrétion. Pour plus d'informations, veuillez consulter la [politique de maintenance des kits SDK et des outils AWS](#) dans le Guide de référence des kits SDK et des outils AWS .

Voici les versions minimales qui prennent en charge IMDSv2 :

- [AWS CLI](#) : 1.16.289
- [AWS Tools for Windows PowerShell](#) – 4.0.1.0
- [AWS SDK for .NET](#) : 3.3.634.1
- [AWS SDK for C++](#) : 1.7.229
- [AWS SDK for Go](#) : 1.25.38
- [AWS SDK pour Go v2](#) — 0.19.0
- [AWS SDK for Java](#) : 1.11.678
- [AWS SDK for Java 2.x](#) : 2.10.21
- [AWS SDK pour Node.js — JavaScript 2.722.0](#)
- [AWS SDK for PHP](#) : 3.147.7
- [AWS SDK pour Python \(Botocore\)](#) — 1.13.25
- [AWS SDK for Python \(Boto3\)](#) : 1.12.6
- [AWS SDK for Ruby](#) : 3.79.0

Configurer les options de métadonnées d'instance

Le service de métadonnées d'instance (IMDS) s'exécute localement sur chaque instance EC2. Les options de métadonnées d'instance font référence à un ensemble de configurations qui contrôlent l'accessibilité et le comportement de l'IMDS sur une instance EC2.

Vous pouvez configurer les options de métadonnées d'instance suivantes sur chaque instance :

Service de métadonnées d'instance (IMDS) : | enabled disabled

Vous pouvez activer ou désactiver l'IMDS sur une instance. Lorsque cette option est désactivée, vous ou aucun code ne pourrez accéder aux métadonnées de l'instance.

L'IMDS possède deux points de terminaison sur une instance : IPv4 (169.254.169.254) et IPv6 (). [fd00:ec2::254] Lorsque vous activez l'IMDS, le point de terminaison IPv4 est automatiquement activé. Si vous souhaitez activer le point de terminaison IPv6, vous devez le faire explicitement.

Point de terminaison IPv6 IMDS : | enabled disabled

Vous pouvez activer explicitement le point de terminaison IPv6 IMDS sur une instance. Lorsque le point de terminaison IPv6 est activé, le point de terminaison IPv4 reste activé. Le point de terminaison IPv6 n'est pris en charge que [sur les instances créées sur le système AWS Nitro](#) et dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement).

Version des métadonnées : IMDSv1 or IMDSv2 (token optional) | IMDSv2 only (token required)

Lors de la demande de métadonnées d'instance, les appels IMDSv2 nécessitent un jeton. Les appels IMDSv1 ne nécessitent pas de jeton. Vous pouvez configurer une instance pour autoriser les appels IMDSv1 ou IMDSv2 (où un jeton est facultatif), ou pour autoriser uniquement les appels IMDSv2 (lorsqu'un jeton est requis).

Limite de sauts de réponse aux métadonnées : 1 — 64

La limite de sauts est le nombre de sauts réseau que la réponse PUT est autorisée à effectuer. Vous pouvez définir la limite de sauts sur un minimum 1 et un maximum de 64. Dans un environnement de conteneurs, nous vous recommandons de définir la limite de sauts sur 2. Pour plus d'informations, consultez [Considérations](#).

Accès aux balises dans les métadonnées de l'instance : enabled | disabled

Vous pouvez activer ou désactiver l'accès aux balises de l'instance à partir des métadonnées d'une instance. Pour plus d'informations, consultez [Utiliser les identifications d'instance dans les métadonnées d'instance](#).

Où configurer les options de métadonnées de l'instance

Les options de métadonnées d'instance peuvent être configurées à différents niveaux, comme suit :

- **Compte** : vous pouvez définir des valeurs par défaut pour les options de métadonnées de l'instance au niveau du compte pour chacune d'entre elles Région AWS. Lorsqu'une instance est lancée, les options de métadonnées de l'instance sont automatiquement définies sur les valeurs au niveau du compte. Vous pouvez modifier ces valeurs au lancement. Les valeurs par défaut au niveau du compte n'affectent pas les instances existantes.

- AMI — Vous pouvez définir le `imds-support` paramètre sur `v2.0` lorsque vous enregistrez ou modifiez une AMI. Lorsqu'une instance est lancée avec cette AMI, la version des métadonnées de l'instance est automatiquement définie sur IMDSv2 et la limite de sauts est définie sur 2.
- Instance : vous pouvez modifier toutes les options de métadonnées d'une instance au lancement, en remplaçant les paramètres par défaut. Vous pouvez également modifier les options de métadonnées de l'instance après le lancement d'une instance en cours d'exécution ou arrêtée. Notez que les modifications peuvent être limitées par une politique IAM ou SCP.

Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance pour les nouvelles instances](#) et [Configurer les options de métadonnées d'instance pour les instances existantes](#).

Ordre de priorité pour les options de métadonnées des instances

La valeur de chaque option de métadonnées d'instance est déterminée lors du lancement de l'instance, selon un ordre de priorité hiérarchique. La hiérarchie, avec la priorité la plus élevée au sommet, est la suivante :

- Priorité 1 : Configuration de l'instance au lancement — Les valeurs peuvent être spécifiées dans le modèle de lancement ou dans la configuration de l'instance. Toutes les valeurs spécifiées ici remplacent les valeurs spécifiées au niveau du compte ou dans l'AMI.
- Priorité 2 : paramètres du compte — Si aucune valeur n'est spécifiée au lancement de l'instance, elle est déterminée par les paramètres au niveau du compte (qui sont définis pour chacun). Région AWS Les paramètres au niveau du compte incluent une valeur pour chaque option de métadonnées ou n'indiquent aucune préférence.
- Priorité 3 : configuration de l'AMI — Si aucune valeur n'est spécifiée au lancement de l'instance ou au niveau du compte, elle est déterminée par la configuration de l'AMI. Cela s'applique uniquement à `HttpTokens` et `HttpPutResponseHopLimit`.

Chaque option de métadonnées est évaluée séparément. L'instance peut être configurée à l'aide d'une combinaison de configuration directe, de paramètres par défaut au niveau du compte et de configuration depuis l'AMI.

Vous pouvez modifier la valeur de n'importe quelle option de métadonnées après le lancement sur une instance en cours d'exécution ou arrêtée, sauf si les modifications sont limitées par une politique IAM ou SCP.

Déterminer les valeurs des options de métadonnées — Exemple 1

Dans cet exemple, une instance EC2 est lancée dans une région où le paramètre `HttpPutResponseHopLimit` est défini 1 au niveau du compte. L'AMI spécifiée est `ImdsSupport` définie `surv2.0`. Aucune option de métadonnées n'est spécifiée directement sur l'instance au lancement. L'instance est lancée avec les options de métadonnées suivantes :

```
"MetadataOptions": {  
  ...  
  "HttpTokens": "required",  
  "HttpPutResponseHopLimit": 1,  
  ...  
}
```

Ces valeurs ont été déterminées comme suit :

- Aucune option de métadonnées spécifiée au lancement : lors du lancement de l'instance, aucune valeur spécifique pour les options de métadonnées n'était fournie ni dans les paramètres de lancement de l'instance ni dans le modèle de lancement.
- Les paramètres du compte ont la priorité suivante : en l'absence de valeurs spécifiques spécifiées au lancement, les paramètres au niveau du compte dans la région sont prioritaires. Cela signifie que les valeurs par défaut configurées au niveau du compte sont appliquées. Dans ce cas, le `HttpPutResponseHopLimit` a été réglé sur 1.
- Les paramètres de l'AMI ont la dernière priorité : en l'absence de valeur spécifique spécifiée au lancement ou au niveau du compte pour `HttpTokens` (la version des métadonnées de l'instance), le paramètre de l'AMI est appliqué. Dans ce cas, le paramètre AMI a `ImdsSupport: v2.0` déterminé que ce paramètre `HttpTokens` était défini `surrequired`. Notez que bien que le paramètre AMI `ImdsSupport: v2.0` soit conçu pour être défini `HttpPutResponseHopLimit: 2`, il a été remplacé par le paramètre au niveau du compte `HttpPutResponseHopLimit: 1`, qui a une priorité plus élevée.

Déterminer les valeurs des options de métadonnées — Exemple 2

Dans cet exemple, l'instance EC2 est lancée avec les mêmes paramètres que dans l'exemple 1 précédent, mais avec la valeur `HttpTokens` définie sur `optional` directement sur l'instance au lancement. L'instance est lancée avec les options de métadonnées suivantes :

```
"MetadataOptions": {  
  ...  
}
```

```
"HttpTokens": "optional",
"HttpPutResponseHopLimit": 1,
...
```

La valeur pour `HttpPutResponseHopLimit` est déterminée de la même manière que dans l'exemple 1. Toutefois, la valeur pour `HttpTokens` est déterminée comme suit : Les options de métadonnées configurées sur l'instance au lancement sont prioritaires. Même si l'AMI était configurée avec `ImdsSupport: v2.0` (en d'autres termes, elle `HttpTokens` est définie `suroptional`), la valeur spécifiée sur l'instance au lancement (`HttpTokens` définie `suroptional`) était prioritaire.

Définissez la version des métadonnées de l'instance

Lorsqu'une instance est lancée, la valeur de la version des métadonnées de l'instance est `IMDSv1` or `IMDSv2 (token optional)` ou `IMDSv2 only (token required)`.

Au lancement de l'instance, vous pouvez soit spécifier manuellement la valeur de la version des métadonnées, soit utiliser la valeur par défaut. Si vous spécifiez manuellement la valeur, elle remplace les valeurs par défaut. Si vous choisissez de ne pas spécifier manuellement la valeur, elle sera déterminée par une combinaison de paramètres par défaut, comme indiqué dans le tableau suivant.

Le tableau montre comment la version des métadonnées d'une instance au lancement (indiquée par Configuration de l'instance résultante dans la colonne 4) est déterminée par les paramètres aux différents niveaux de configuration. L'ordre de priorité est de gauche à droite, la première colonne ayant la priorité la plus élevée, comme suit :

- Colonne 1 : paramètre de lancement : représente le paramètre de l'instance que vous spécifiez manuellement au lancement.
- Colonne 2 : Niveau de compte par défaut — Représente le paramètre du compte.
- Colonne 3 : valeur par défaut de l'AMI — Représente le paramètre de l'AMI.

Paramètre de lancement	Niveau de compte par défaut	AMI par défaut	Configuration de l'instance résultante
V2 uniquement (jeton requis)	Aucune préférence	V2 uniquement	V2 uniquement

Paramètre de lancement	Niveau de compte par défaut	AMI par défaut	Configuration de l'instance résultante
V2 uniquement (jeton requis)	V2 uniquement	V2 uniquement	V2 uniquement
V2 uniquement (jeton requis)	V1 ou V2	V2 uniquement	V2 uniquement
V1 ou V2 (jeton facultatif)	Aucune préférence	V2 uniquement	V1 ou V2
V1 ou V2 (jeton facultatif)	V2 uniquement	V2 uniquement	V1 ou V2
V1 ou V2 (jeton facultatif)	V1 ou V2	V2 uniquement	V1 ou V2
Non défini	Aucune préférence	V2 uniquement	V2 uniquement
Non défini	V2 uniquement	V2 uniquement	V2 uniquement
Non défini	V1 ou V2	V2 uniquement	V1 ou V2
V2 uniquement (jeton requis)	Aucune préférence	null	V2 uniquement
V2 uniquement (jeton requis)	V2 uniquement	null	V2 uniquement
V2 uniquement (jeton requis)	V1 ou V2	null	V2 uniquement
V1 ou V2 (jeton facultatif)	Aucune préférence	null	V1 ou V2
V1 ou V2 (jeton facultatif)	V2 uniquement	null	V1 ou V2

Paramètre de lancement	Niveau de compte par défaut	AMI par défaut	Configuration de l'instance résultante
V1 ou V2 (jeton facultatif)	V1 ou V2	null	V1 ou V2
Non défini	Aucune préférence	null	V1 ou V2
Non défini	V2 uniquement	null	V2 uniquement
Non défini	V1 ou V2	null	V1 ou V2

Utiliser les clés de condition IAM pour restreindre les options de métadonnées de l'instance

Vous pouvez utiliser les clés de condition IAM dans une politique IAM ou un SCP comme suit :

- Autoriser le lancement d'une instance uniquement si elle est configurée pour exiger l'utilisation d'IMDSv2
- Restreindre le nombre de sauts autorisés
- Désactiver l'accès aux métadonnées d'instance

Tâches

- [Configurer les options de métadonnées d'instance pour les nouvelles instances](#)
- [Configurer les options de métadonnées d'instance pour les instances existantes](#)

Note

Vous devez procéder avec précautions et effectuer des tests méticuleux avant toute modification. Notez les informations suivantes :

- Si vous imposez l'utilisation de IMDSv2, les applications ou agents qui utilisent IMDSv1 pour l'accès aux métadonnées d'instance cesseront de fonctionner.
- Si vous désactivez tous les accès aux métadonnées d'instance, les applications ou agents dont le fonctionnement repose sur l'accès aux métadonnées d'instance cesseront de fonctionner.

- Pour IMDSv2, vous devez utiliser `/latest/api/token` lors de la récupération du jeton.
- (Windows uniquement) Si votre PowerShell version est antérieure à 4.0, vous devez effectuer la [mise à jour vers Windows Management Framework 4.0](#) pour exiger l'utilisation d'IMDSv2.

Configurer les options de métadonnées d'instance pour les nouvelles instances

Vous pouvez configurer les options de métadonnées d'instance suivantes pour les nouvelles instances.

Options

- [Exigence d'utilisation d'IMDSv2](#)
- [Activer les points de terminaison IPv4 et IPv6 de l'IMDS](#)
- [Désactiver l'accès aux métadonnées d'instance](#)

Exigence d'utilisation d'IMDSv2

Vous pouvez utiliser les méthodes suivantes pour exiger l'utilisation d'IMDSv2 sur vos nouvelles instances.

Pour exiger IMDSv2

- [Définissez IMDSv2 comme valeur par défaut pour le compte](#)
- [Configurer l'instance au lancement](#)
- [Configurer l'AMI](#)
- [Utiliser une politique IAM](#)

Définissez IMDSv2 comme valeur par défaut pour le compte

Vous pouvez définir la version par défaut du service de métadonnées d'instance (IMDS) au niveau du compte pour chacun Région AWS d'entre eux. Cela signifie que lorsque vous lancez une nouvelle instance, la version des métadonnées de l'instance est automatiquement définie sur la valeur par défaut au niveau du compte. Toutefois, vous pouvez modifier manuellement la valeur au lancement ou après le lancement. Pour plus d'informations sur la manière dont les paramètres au niveau du compte et les remplacements manuels affectent une instance, consultez. [Ordre de priorité pour les options de métadonnées des instances](#)

Note

La définition de la valeur par défaut au niveau du compte ne réinitialise pas les instances existantes. Par exemple, si vous définissez la valeur par défaut du compte sur IMDSv2, les instances existantes définies sur IMDSv1 ne sont pas affectées. Si vous souhaitez modifier la valeur des instances existantes, vous devez modifier manuellement la valeur des instances elles-mêmes.

Vous pouvez définir le compte par défaut pour la version des métadonnées de l'instance sur IMDSv2 afin que toutes les nouvelles instances du compte soient lancées avec IMDSv2, et IMDSv1 soit désactivé. Avec ce compte par défaut, lorsque vous lancez une instance, les valeurs par défaut de l'instance sont les suivantes :

- Console : la version des métadonnées est définie sur V2 uniquement (jeton requis) et la limite de sauts de réponse des métadonnées est définie sur 2.
- AWS CLI: `HttpTokens` est défini sur `required` et `HttpPutResponseHopLimit` est défini sur 2.

Note

Avant de définir le compte par défaut sur IMDSv2, assurez-vous que vos instances ne dépendent pas d'IMDSv1. Pour plus d'informations, consultez [Chemin recommandé pour demander l'accès à IMDSv2](#).

Console

Pour définir IMDSv2 comme compte par défaut pour la région spécifiée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Tableau de bord du EC2.
4. Sous Attributs du compte, sélectionnez Protection et sécurité des données.
5. À côté des paramètres IMDS par défaut, choisissez Gérer.
6. Sur la page Gérer les paramètres par défaut de l'IMDS, procédez comme suit :

- a. Pour le service de métadonnées d'instance, choisissez Enabled.
- b. Pour Choisir une version des métadonnées, sélectionnez V2 (jeton obligatoire).
- c. Pour la limite de sauts de réponse aux métadonnées, spécifiez 2 si vos instances hébergeront des conteneurs. Sinon, sélectionnez Aucune préférence. Lorsqu'aucune préférence n'est spécifiée, au lancement, la valeur par défaut est 2 si l'AMI nécessite IMDSv2 ; sinon, elle est définie par défaut sur 1.
- d. Choisissez Mettre à jour.

AWS CLI

Pour définir IMDSv2 comme compte par défaut pour la région spécifiée

Utilisez la commande [modify-instance-metadata-defaults](#) et spécifiez la région dans laquelle vous souhaitez modifier les paramètres au niveau du compte IMDS. Incluez `--http-tokens set to required` et `--http-put-response-hop-limit set to 2` si vos instances hébergeront des conteneurs. Dans le cas contraire, spécifiez `-1` pour n'indiquer aucune préférence. Lorsque `-1` (aucune préférence) est spécifiée, au lancement, la valeur par défaut est 2 si l'AMI nécessite IMDSv2 ; sinon, elle est définie par défaut sur 1.

```
aws ec2 modify-instance-metadata-defaults \  
  --region us-east-1 \  
  --http-tokens required \  
  --http-put-response-hop-limit 2
```

Sortie attendue

```
{  
  "Return": true  
}
```

Pour afficher les paramètres de compte par défaut pour les options de métadonnées de l'instance pour la région spécifiée

Utilisez la [get-instance-metadata-defaults](#) commande et spécifiez la région.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Exemple de sortie

```
{
  "AccountLevel": {
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 2
  }
}
```

Configurer l'instance au lancement

Quand vous [lancez une instance](#), vous pouvez configurer l'instance pour imposer l'utilisation de IMDSv2 en configurant les champs suivants :

- Console Amazon EC2 : définissez Metadata version (Version des métadonnées) sur V2 only (token required) (V2 uniquement [jeton obligatoire]).
- AWS CLI : définissez HttpTokens sur `required`.

Lorsque vous spécifiez que IMDSv2 est requis, vous devez également activer le point de terminaison du service des métadonnées d'instance (IMDS) en définissant Métadonnées accessibles sur Activé (console) ou `HttpEndpoint` sur `enabled` (AWS CLI).

Dans un environnement de conteneur, lorsque IMDSv2 est requis, nous vous recommandons de définir la limite de sauts sur `2`. Pour plus d'informations, consultez [Considérations](#).

New console

Pour imposer l'utilisation d'IMDSv2 sur une nouvelle instance

- Lors du lancement d'une nouvelle instance dans la console Amazon EC2, développez Détails avancés, et procédez comme suit :
 - Pour Accéder aux métadonnées, choisissez Activé.
 - Pour Choisir une version des métadonnées, sélectionnez V2 (jeton obligatoire).
 - (Environnement de conteneur) Pour Limite de sauts de réponse aux métadonnées, choisissez 2.

Pour plus d'informations, consultez [Détails avancés](#).

Old console

Pour imposer l'utilisation d'IMDSv2 sur une nouvelle instance

- Lors du lancement d'une nouvelle instance dans la console Amazon EC2, sélectionnez les options suivantes sur la page Configurer les détails de l'instance :
 - Sous Détails avancés, pour Métadonnées accessibles, sélectionnez Activé.
 - Pour Version des métadonnées, sélectionnez V2 (jeton obligatoire).

Pour plus d'informations, consultez [Étape 3 : Configurer les détails de l'instance](#).

AWS CLI

Pour imposer l'utilisation d'IMDSv2 sur une nouvelle instance

L'exemple [run-instances](#) ci-dessous lance une instance `c6i.large` avec `--metadata-options` défini sur `HttpTokens=required`. Lorsque vous spécifiez une valeur pour `HttpTokens`, vous devez également définir `HttpEndpoint` sur `enabled`. Comme l'en-tête de jeton sécurisé est défini sur `required` pour les demandes de récupération de métadonnées, cette option impose à l'instance l'utilisation de IMDSv2 lors de la demande des métadonnées d'instance.

Dans un environnement de conteneur, lorsque IMDSv2 est requis, nous recommandons de définir la limite de sauts sur `with. 2 HttpPutResponseHopLimit=2`

```
aws ec2 run-instances \  
  --image-id ami-0abcdef1234567890 \  
  --instance-type c6i.large \  
  ...  
  --metadata-options  
  "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

Pour imposer l'utilisation d'IMDSv2 sur une nouvelle instance

L'exemple d'[New-EC2Instance](#) applet de commande suivant lance une `c6i.large` instance dont le paramètre est `MetadataOptions_HttpEndpoint` défini sur `enabled` et le `MetadataOptions_HttpTokens` paramètre sur `required`. Lorsque vous spécifiez une valeur

pour `HttpTokens`, vous devez également définir `HttpEndpoint` sur `enabled`. Comme l'en-tête de jeton sécurisé est défini sur `required` pour les demandes de récupération de métadonnées, cette option impose à l'instance l'utilisation de IMDSv2 lors de la demande des métadonnées d'instance.

```
New-EC2Instance `
  -ImageId ami-0abcdef1234567890 `
  -InstanceType c6i.large `
  -MetadataOptions_HttpEndpoint enabled `
  -MetadataOptions_HttpTokens required
```

AWS CloudFormation

Pour spécifier les options de métadonnées pour une instance utilisant AWS CloudFormation, consultez la [AWS::EC2::LaunchTemplate MetadataOptions](#) propriété dans le guide de AWS CloudFormation l'utilisateur.

Configurer l'AMI

Lorsque vous enregistrez une nouvelle AMI ou que vous modifiez une AMI existante, vous pouvez définir le paramètre `imds-support` sur `v2.0`. Les instances lancées à partir de cette AMI verront le paramètre `Metadata version` (Version des métadonnées) défini sur `V2 only (token required)` (V2 uniquement [jeton obligatoire]) (console) ou `HttpTokens` défini sur `required` (AWS CLI). Avec ces paramètres, l'instance impose l'utilisation de IMDSv2 lors de la demande de métadonnées d'instance.

Notez que lorsque vous définissez `imds-support` sur `v2.0`, les instances lancées à partir de cette AMI verront également le paramètre `Metadata response hop limit` (Limite de saut de réponse des métadonnées) (console) ou `http-put-response-hop-limit` (AWS CLI) défini sur `2`.

Important

N'utilisez ce paramètre que si votre logiciel AMI prend en charge IMDSv2. Une fois que vous avez défini la valeur sur `v2.0`, vous ne pouvez pas revenir en arrière. La seule façon de « réinitialiser » votre AMI est de créer une nouvelle AMI à partir de l'instantané sous-jacent.

Configuration d'une nouvelle AMI pour IMDSv2

Utilisez l'une des méthodes suivantes pour configurer une nouvelle AMI pour IMDSv2.

AWS CLI

L'exemple [register-image](#) suivant enregistre une AMI en utilisant l'instantané spécifié d'un volume racine EBS en tant que périphérique `/dev/xvda`. Spécifiez `v2.0` pour le paramètre `imds-support`, de sorte que les instances lancées à partir de cette AMI imposent l'utilisation de IMDSv2 pour pouvoir demander des métadonnées d'instance.

```
aws ec2 register-image \  
  --name my-image \  
  --root-device-name /dev/xvda \  
  --block-device-mappings DeviceName=/dev/  
xvda,Ebs={SnapshotId=snap-0123456789example} \  
  --architecture x86_64 \  
  --imds-support v2.0
```

PowerShell

L'exemple de [Register-EC2Image](#) cmdlet suivant enregistre une AMI en utilisant l'instantané spécifié d'un volume racine EBS en tant que périphérique `/dev/xvda`. Spécifiez `v2.0` pour le paramètre `ImdsSupport`, de sorte que les instances lancées à partir de cette AMI imposent l'utilisation de IMDSv2 pour pouvoir demander des métadonnées d'instance.

```
Import-Module AWS.Tools.EC2 # Required for Amazon.EC2.Model object creation.  
Register-EC2Image `br/>  -Name 'my-image' `br/>  -RootDeviceName /dev/xvda `br/>  -BlockDeviceMapping (  
    New-Object `br/>      -TypeName Amazon.EC2.Model.BlockDeviceMapping `br/>      -Property @{  
        DeviceName = '/dev/xvda';  
        EBS = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property  
@{  
          SnapshotId = 'snap-0123456789example;  
          VolumeType = 'gp3'  
        } )  
      } ) `br/>  -Architecture X86_64 `br/>  -ImdsSupport v2.0
```

Configuration d'une AMI existante pour IMDSv2

Pour configurer une AMI existante pour IMDSv2, utilisez l'une des méthodes suivantes.

AWS CLI

L'exemple [modify-image-attribute](#) suivant modifie une AMI existante pour IMDSv2 uniquement. Spécifiez `v2.0` pour le paramètre `imds-support`, de sorte que les instances lancées à partir de cette AMI imposent l'utilisation de IMDSv2 pour pouvoir demander des métadonnées d'instance.

```
aws ec2 modify-image-attribute \  
  --image-id ami-0123456789example \  
  --imds-support v2.0
```

PowerShell

L'exemple de [Edit-EC2ImageAttribute](#) cmdlet suivant modifie une AMI existante pour IMDSv2 uniquement. Spécifiez `v2.0` pour le paramètre `imds-support`, de sorte que les instances lancées à partir de cette AMI imposent l'utilisation de IMDSv2 pour pouvoir demander des métadonnées d'instance.

```
Edit-EC2ImageAttribute \  
  -ImageId ami-0abcdef1234567890 \  
  -ImdsSupport 'v2.0'
```

Utiliser une politique IAM

Vous pouvez créer une politique IAM qui empêche les utilisateurs de lancer de nouvelles instances qui n'utilisent pas IMDSv2.

Pour imposer l'utilisation de IMDSv2 sur toutes les nouvelles instances en utilisant une politique IAM

Pour vous assurer que les utilisateurs peuvent uniquement lancer les instances nécessitant l'utilisation de IMDSv2 lors de la demande de métadonnées d'instance, vous pouvez spécifier que la condition imposant l'utilisation de IMDSv2 devra être remplie pour qu'une instance puisse être lancée. Pour examiner l'exemple de stratégie IAM, consultez [Utiliser des métadonnées d'instance](#).

Activer les points de terminaison IPv4 et IPv6 de l'IMDS

L'IMDS possède deux points de terminaison sur une instance : IPv4 (169.254.169.254) et IPv6 ([fd00:ec2::254]). Lorsque vous activez l'IMDS, le point de terminaison IPv4 est automatiquement

activé. Le point de terminaison IPv6 reste désactivé même si vous lancez une instance dans un sous-réseau IPv6 uniquement. Pour activer le point de terminaison IPv6, vous devez le faire explicitement. Lorsque vous activez le point de terminaison IPv6, le point de terminaison IPv4 reste activé.

Vous pouvez activer le point de terminaison IPv6 au lancement de l'instance ou après.

Conditions requises pour activer le point de terminaison IPv6

- Le type d'instance sélectionné est basé sur le [système AWS Nitro](#).
- Le sous-réseau sélectionné prend en charge le protocole IPv6, le sous-réseau étant soit à [double pile, soit uniquement IPv6](#).

Utilisez l'une des méthodes suivantes pour lancer une instance avec le point de terminaison IPv6 IMDS activé.

New console

Pour activer le point de terminaison IPv6 IMDS lors du lancement de l'instance

- [Lancez l'instance](#) dans la console Amazon EC2 avec les informations suivantes spécifiées sous Advanced details (Détails avancés) :
 - Pour le point de terminaison IPv6 des métadonnées, choisissez Enabled.

Pour plus d'informations, consultez [Détails avancés](#).

AWS CLI

Pour activer le point de terminaison IPv6 IMDS lors du lancement de l'instance

L'exemple [run-instances](#) suivant lance une instance `c6i.large` avec le point de terminaison IPv6 activé pour l'IMDS. Pour activer le point de terminaison IPv6, pour le paramètre `--metadata-options`, spécifiez `HttpProtocolIpv6=enabled`. Lorsque vous spécifiez une valeur pour `HttpProtocolIpv6`, vous devez également définir `HttpEndpoint` sur `enabled`.

```
aws ec2 run-instances \  
  --image-id ami-0abcdef1234567890 \  
  --instance-type c6i.large \  
  ...  
  --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Pour activer le point de terminaison IPv6 IMDS lors du lancement de l'instance

L'exemple d'[New-EC2Instance](#) applet de commande suivant lance une `c6i.large` instance avec le point de terminaison IPv6 activé pour l'IMDS. Pour activer le point de terminaison IPv6, définissez `MetadataOptions_HttpProtocolIpv6` sur `enabled`. Lorsque vous spécifiez une valeur pour `MetadataOptions_HttpProtocolIpv6`, vous devez également définir `MetadataOptions_HttpEndpoint` sur `enabled`.

```
New-EC2Instance `
  -ImageId ami-0abcdef1234567890 `
  -InstanceType c6i.large `
  -MetadataOptions_HttpEndpoint enabled `
  -MetadataOptions_HttpProtocolIpv6 enabled
```

Désactiver l'accès aux métadonnées d'instance

Vous pouvez désactiver l'accès aux métadonnées de l'instance en désactivant l'IMDS lorsque vous lancez une instance. Vous pouvez activer l'accès ultérieurement en réactivant l'IMDS. Pour plus d'informations, consultez [Activer l'accès aux métadonnées d'instance](#).

Important

Vous pouvez choisir de désactiver l'IMDS au lancement ou après le lancement. Si vous désactivez l'IMDS au lancement, les opérations suivantes risquent de ne pas fonctionner :

- Vous pourriez ne pas avoir d'accès SSH à votre instance. La `public-keys/0/openssh-key`, qui est la clé SSH publique de votre instance, ne sera pas accessible, car elle est normalement fournie et accessible à partir des métadonnées de l'instance EC2.
- Les données utilisateur EC2 ne seront pas disponibles et ne seront pas exécutées au démarrage de l'instance. Les données utilisateur EC2 sont hébergées sur l'IMDS. Si vous désactivez l'IMDS, vous empêchez l'accès aux données utilisateur.

Pour accéder à cette fonctionnalité, vous pouvez réactiver l'IMDS après le lancement.

New console

Pour désactiver l'accès aux métadonnées d'instance

- [Lancez l'instance](#) dans la console Amazon EC2 avec les informations suivantes spécifiées sous Advanced details (Détails avancés) :
 - Pour accéder aux métadonnées, choisissez Activé.

Pour plus d'informations, consultez [Détails avancés](#).

Old console

Pour désactiver l'accès aux métadonnées d'instance

- Lancez l'instance dans la console Amazon EC2 avec l'option suivante sélectionnée sur la page Configure Instance Details (Configurer les détails de l'instance) :
 - Sous Détails avancés, pour Métadonnées accessibles, sélectionnez Désactivé.

Pour plus d'informations, consultez [Étape 3 : Configurer les détails de l'instance](#).

AWS CLI

Pour désactiver l'accès aux métadonnées d'instance au lancement

Lancez l'instance avec `--metadata-options` défini sur `HttpEndpoint=disabled`.

```
aws ec2 run-instances \  
  --image-id ami-0abcdef1234567890 \  
  --instance-type c6i.large \  
  ...  
  --metadata-options "HttpEndpoint=disabled"
```

PowerShell

Pour désactiver l'accès aux métadonnées d'instance au lancement

L'exemple d'[New-EC2Instance](#) applet de commande suivant lance une instance dont la valeur est `MetadataOptions_HttpEndpoint` définie sur `disabled`

```
New-EC2Instance `
```

```
-ImageId ami-0abcdef1234567890 `
-InstanceType c6i.large `
-MetadataOptions_HttpEndpoint disabled
```

AWS CloudFormation

Pour spécifier les options de métadonnées pour une instance utilisant AWS CloudFormation, consultez la [AWS::EC2::LaunchTemplate MetadataOptions](#) propriété dans le guide de AWS CloudFormation l'utilisateur.

Configurer les options de métadonnées d'instance pour les instances existantes

Vous pouvez modifier les options des métadonnées d'instance pour les instances existantes.

De même, vous pouvez créer une politique IAM qui empêche les utilisateurs de modifier les options des métadonnées d'instance sur des instances existantes. Pour contrôler quels utilisateurs peuvent modifier les options de métadonnées de l'instance, spécifiez une politique qui empêche tous les utilisateurs autres que les utilisateurs ayant un rôle spécifique d'utiliser l'[ModifyInstanceMetadataOptions](#) API. Pour examiner l'exemple de stratégie IAM, consultez [Utiliser des métadonnées d'instance](#).

Interroger les options de métadonnées d'instance pour les instances existantes

Vous pouvez interroger les options de métadonnées d'instance pour vos instances existantes en utilisant l'une des méthodes suivantes.

Console

Pour interroger les options de métadonnées d'instance pour une instance existante à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez votre instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Passez en revue les options de métadonnées d'instance actuelles dans la boîte de dialogue Modifier les options de métadonnées d'instance.

AWS CLI

Pour interroger les options de métadonnées d'instance pour une instance existante à l'aide du AWS CLI

Utilisez la commande [describe-instances](#) de l'interface de ligne de commande.

```
aws ec2 describe-instances \  
  --instance-id i-1234567898abcdef0 \  
  --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Pour interroger les options de métadonnées d'instance pour une instance existante à l'aide des outils de PowerShell

Utilisez l'[Get-EC2Instance](#) applet de commande.

```
(Get-EC2Instance \  
  -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Exigence d'utilisation d'IMDSv2

Utilisez l'une des méthodes suivantes pour modifier les options des métadonnées d'instance sur une instance existante afin d'imposer l'utilisation d'IMDSv2 pour pouvoir demander des métadonnées d'instance. Lorsque IMDSv2 est requis, IMDSv1 ne peut pas être utilisé.

Note

Avant de demander l'utilisation d'IMDSv2, assurez-vous que l'instance n'effectue pas d'appels IMDSv1. La `MetadataNoToken` CloudWatch métrique suit les appels IMDSv1. Lorsqu'aucune `MetadataNoToken` utilisation d'IMDSv1 n'est enregistrée pour une instance, celle-ci est alors prête à nécessiter IMDSv2.

Console

Imposition de l'utilisation d'IMDSv2 sur une instance existante

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez votre instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Dans la boîte de dialogue Modifier les options des métadonnées d'instance, procédez comme suit :
 - a. Pour Service de métadonnées d'instance, sélectionnez Activer.
 - b. Pour IMDSv2, choisissez Requis.
 - c. Choisissez Enregistrer.

AWS CLI

Imposition de l'utilisation d'IMDSv2 sur une instance existante

Utilisez la commande d'interface de ligne de commande [modify-instance-metadata-options](#) et définissez le paramètre `http-tokens` sur `required`. Lorsque vous spécifiez une valeur pour `http-tokens`, vous devez également définir `http-endpoint` sur `enabled`.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-tokens required \  
  --http-endpoint enabled
```

PowerShell

Imposition de l'utilisation d'IMDSv2 sur une instance existante

Utilisez l'[Edit-EC2InstanceMetadataOption](#) applet de commande et définissez le `HttpTokens` paramètre sur `required`. Lorsque vous spécifiez une valeur pour `HttpTokens`, vous devez également définir `HttpEndpoint` sur `enabled`.

```
(Edit-EC2InstanceMetadataOption \  
  -InstanceId i-1234567898abcdef0 \  
  -HttpTokens required \  
  -HttpEndpoint enabled).InstanceMetadataOptions
```

Restaurer l'utilisation d'IMDSv1

Lorsque IMDSv2 est requis, IMDSv1 ne fonctionne pas lors de la demande de métadonnées d'instance. Lorsque IMDSv2 est facultatif, IMDSv2 et IMDSv1 fonctionnent. Par conséquent, pour restaurer IMDSv1, rendez IMDSv2 facultatif en utilisant l'une des méthodes suivantes.

Console

Restauration de l'utilisation d'IMDSv1 sur une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez votre instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Dans la boîte de dialogue Modifier les options des métadonnées d'instance, procédez comme suit :
 - a. Pour Service de métadonnées d'instance, assurez-vous que l'option Activer est sélectionnée.
 - b. Pour IMDSv2, choisissez Facultatif.
 - c. Choisissez Enregistrer.

AWS CLI

Restauration de l'utilisation d'IMDSv1 sur une instance

Vous pouvez utiliser la commande de l'interface de ligne de commande [modify-instance-metadata-options](#) avec `http-tokens` défini sur `optional` pour restaurer l'utilisation de IMDSv1 lors de la demande de métadonnées d'instance.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-tokens optional \  
  --http-endpoint enabled
```

PowerShell

Restauration de l'utilisation d'IMDSv1 sur une instance

Vous pouvez utiliser l'[Edit-EC2InstanceMetadataOption](#) applet de commande avec `HttpTokens optional` pour rétablir l'utilisation d'IMDSv1 lors de la demande de métadonnées d'instance.

```
(Edit-EC2InstanceMetadataOption \  
  -InstanceId i-1234567898abcdef0 \  
  -HttpTokens optional \  
  -HttpEndpoint enabled).InstanceMetadataOptions
```

Modifier la durée de vie de la réponse PUT

Pour les instances existantes, vous pouvez modifier les paramètres de la durée de vie (hop limit) de la réponse PUT.

Actuellement, seuls les AWS SDK AWS CLI et prennent en charge la modification de la limite de sauts de réponse PUT.

AWS CLI

Pour modifier la durée de vie (hop limit) de la réponse PUT

Utilisez la commande d'interface de ligne de commande [modify-instance-metadata-options](#) et définissez le paramètre `http-put-response-hop-limit` sur la durée de vie (hop limit) requise. Dans l'exemple suivant, la durée de vie (hop limit) est définie 3. Notez que lorsque vous spécifiez une valeur pour `http-put-response-hop-limit`, vous devez également définir `http-endpoint` sur `enabled`.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-put-response-hop-limit 3 \  
  --http-endpoint enabled
```

PowerShell

Pour modifier la durée de vie (hop limit) de la réponse PUT

Utilisez l'[Edit-EC2InstanceMetadataOption](#) applet de commande et définissez le `HttpPutResponseHopLimit` paramètre sur le nombre de sauts requis. Dans l'exemple suivant, la durée de vie (hop limit) est définie 3. Notez que lorsque vous spécifiez une valeur pour `HttpPutResponseHopLimit`, vous devez également définir `HttpEndpoint` sur `enabled`.

```
(Edit-EC2InstanceMetadataOption \  
  -InstanceId i-1234567898abcdef0 \  
  -HttpPutResponseHopLimit 3 \  
  -HttpEndpoint enabled).InstanceMetadataOptions
```

Activer les points de terminaison IPv4 et IPv6 de l'IMDS

L'IMDS possède deux points de terminaison sur une instance : IPv4 (169.254.169.254) et IPv6 ([fd00:ec2::254]). Lorsque vous activez l'IMDS, le point de terminaison IPv4 est automatiquement activé. Le point de terminaison IPv6 reste désactivé même si vous lancez une instance dans un sous-réseau IPv6 uniquement. Pour activer le point de terminaison IPv6, vous devez le faire explicitement. Lorsque vous activez le point de terminaison IPv6, le point de terminaison IPv4 reste activé.

Vous pouvez activer le point de terminaison IPv6 au lancement de l'instance ou après.

Conditions requises pour activer le point de terminaison IPv6

- Le type d'instance sélectionné est basé sur le [système AWS Nitro](#).
- Le sous-réseau sélectionné prend en charge le protocole IPv6, le sous-réseau étant soit à [double pile, soit uniquement IPv6](#).

Actuellement, seuls les AWS SDK AWS CLI et prennent en charge l'activation du point de terminaison IPv6 IMDS après le lancement de l'instance.

AWS CLI

Pour activer le point de terminaison IPv6 IMDS pour votre instance

Utilisez la commande d'interface de ligne de commande [modify-instance-metadata-options](#) et définissez le paramètre `http-protocol-ipv6` sur `enabled`. Notez que lorsque vous spécifiez une valeur pour `http-protocol-ipv6`, vous devez également définir `http-endpoint` sur `enabled`.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-protocol-ipv6 enabled \  
  --http-endpoint enabled
```

PowerShell

Pour activer le point de terminaison IPv6 IMDS pour votre instance

Utilisez l'[Edit-EC2InstanceMetadataOption](#) applet de commande et définissez le `HttpProtocolIpv6` paramètre sur `enabled`. Notez que lorsque vous spécifiez une valeur pour `HttpProtocolIpv6`, vous devez également définir `HttpEndpoint` sur `enabled`.

```
(Edit-EC2InstanceMetadataOption `
  -InstanceId i-1234567898abcdef0 `
  -HttpProtocolIpv6 enabled `
  -HttpEndpoint enabled).InstanceMetadataOptions
```

Activer l'accès aux métadonnées d'instance

Vous pouvez activer l'accès aux métadonnées d'instance en activant le point de terminaison HTTP de l'IMDS sur votre instance, quelle que soit la version de ce dernier que vous utilisez. Vous pouvez annuler cette modification à tout moment en désactivant à nouveau le point de terminaison HTTP.

Pour activer l'accès aux métadonnées d'instance sur une instance, utilisez l'une des méthodes suivantes.

Console

Activation de l'accès aux métadonnées d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez votre instance.
4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Dans la boîte de dialogue Modifier les options des métadonnées d'instance, procédez comme suit :
 - a. Pour Service de métadonnées d'instance, sélectionnez Activer.
 - b. Choisissez Enregistrer.

AWS CLI

Activation de l'accès aux métadonnées d'instance

Utilisez la commande d'interface de ligne de commande [modify-instance-metadata-options](#) et définissez le paramètre `http-endpoint` sur `enabled`.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-endpoint enabled
```

PowerShell

Activation de l'accès aux métadonnées d'instance

Utilisez l'[Edit-EC2InstanceMetadataOption](#) applet de commande et définissez le `HttpEndpoint` paramètre sur `enabled`

```
(Edit-EC2InstanceMetadataOption \  
  -InstanceId i-1234567898abcdef0 \  
  -HttpEndpoint enabled).InstanceMetadataOptions
```

Désactiver l'accès aux métadonnées d'instance

Vous pouvez désactiver l'accès aux métadonnées d'instance en désactivant le point de terminaison HTTP de l'IMDS sur votre instance, quelle que soit la version de ce dernier que vous utilisez. Vous pouvez annuler cette modification à tout moment en activant à nouveau le point de terminaison HTTP.

Pour désactiver l'accès aux métadonnées d'instance sur une instance, utilisez l'une des méthodes suivantes.

Console

Désactivation de l'accès aux métadonnées d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez votre instance.

4. Choisissez Actions, Paramètres de l'instance, puis Modifier les options des métadonnées d'instance.
5. Dans la boîte de dialogue Modifier les options des métadonnées d'instance, procédez comme suit :
 - a. Pour Service de métadonnées d'instance, désélectionnez Activer.
 - b. Choisissez Enregistrer.

AWS CLI

Désactivation de l'accès aux métadonnées d'instance

Utilisez la commande d'interface de ligne de commande [modify-instance-metadata-options](#) et définissez le paramètre `http-endpoint` sur `disabled`.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-endpoint disabled
```

PowerShell

Désactivation de l'accès aux métadonnées d'instance

Utilisez l'[Edit-EC2InstanceMetadataOption](#) applet de commande et définissez le `HttpEndpoint` paramètre sur `disabled`

```
(Edit-EC2InstanceMetadataOption \  
  -InstanceId i-1234567898abcdef0 \  
  -HttpEndpoint disabled).InstanceMetadataOptions
```

Récupérer des métadonnées d'instance

Puisque vos métadonnées d'instance sont disponibles à partir de votre instance en cours d'exécution, vous n'avez pas besoin d'utiliser la console Amazon EC2, ni la AWS CLI. Cela peut être utile lorsque vous écrivez des scripts à exécuter depuis votre instance. Par exemple, vous pouvez accéder à l'adresse IP locale de votre instance à partir des métadonnées d'instance afin de gérer une connexion à une application externe.

Les métadonnées d'instance sont divisées en plusieurs catégories. Pour obtenir une description de chaque catégorie de métadonnées d'instance, consultez [Catégories de métadonnées d'instance](#).

Pour voir toutes les catégories de métadonnées d'instance depuis une instance en cours d'exécution, utilisez l'URI IPv4 ou IPv6 ci-après.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Les adresses IP sont des adresses de lien local et sont uniquement valables à partir de l'instance. Pour plus d'informations, consultez [Adresses lien-local](#) dans ce guide de l'utilisateur et l'article [Adresse lien-local](#) (français non garanti) sur Wikipédia.

Note

Les exemples de cette section utilisent l'adresse IPv4 de l'IMDS : 169.254.169.254. Si vous récupérez des métadonnées d'instance pour les instances EC2 sur l'adresse IPv6, assurez-vous d'activer et d'utiliser l'adresse IPv6 à la place : [fd00:ec2::254]. L'adresse IPv6 de l'IMDS est compatible avec les commandes IMDSv2. L'adresse IPv6 n'est accessible que sur [les instances créées sur le système AWS Nitro](#) et dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement).

Le format de la commande est différent selon que vous utilisez IMDSv1 ou IMDSv2. Par défaut, vous pouvez utiliser les deux versions de l'IMDS. Pour imposer l'utilisation de IMDSv2, consultez [Utiliser IMDSv2](#).

Pour récupérer les métadonnées d'instance sur des instances Linux

Vous pouvez utiliser un outil tel que cURL, comme illustré dans l'exemple suivant.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

Pour récupérer les métadonnées d'instance sur des instances Windows

Vous pouvez utiliser des PowerShell applets de commande pour récupérer l'URI. Par exemple, si vous exécutez la version 3.0 ou une version ultérieure de PowerShell, utilisez l'applet de commande suivante.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
```

Si vous ne souhaitez pas l'utiliser PowerShell, vous pouvez installer un outil tiers tel que GNU Wget ou cURL.

Important

Si vous installez un outil tiers sur une instance Windows, assurez-vous de lire avec attention la documentation fournie car la méthode d'appel du HTTP et le format de sortie peuvent être différents de ce qui figure dans la présente documentation.

Coûts

Vous n'êtes pas facturé pour les requêtes HTTP utilisées pour récupérer les métadonnées d'instance et les données utilisateur.

Considérations

Pour éviter les problèmes liés à la récupération des métadonnées d'instance, tenez compte de ce qui suit :

- Dans un environnement de conteneurs, nous vous recommandons de fixer la limite de saut à 2.

Les AWS SDK utilisent les appels IMDSv2 par défaut. Si l'appel IMDSv2 ne reçoit aucune réponse, le kit SDK tente de nouveau l'appel et, s'il échoue à nouveau, utilise IMDSv1. Cela peut entraîner un retard, en particulier dans un environnement de conteneurs. Dans un environnement de conteneur, si la limite de saut est de 1, la réponse de IMDSv2 ne revient pas car un aller vers le conteneur est considéré comme un saut réseau supplémentaire. Pour éviter le processus de retour vers IMDSv1 et le retard qui en résulte, dans un environnement de conteneur, nous vous recommandons de définir la limite de saut à 2. Pour plus d'informations, consultez [Configurer les options de métadonnées d'instance](#).

- (Windows uniquement) Créez des AMI personnalisées avec Windows Sysprep.

Pour garantir le fonctionnement de l'IMDS lorsque vous lancez une instance à partir d'une AMI Windows personnalisée, l'AMI doit être une image standardisée créée avec Windows Sysprep. Sinon, l'IMDS ne fonctionnera pas. Pour plus d'informations, voir [Création d'une AMI avec Windows Sysprep](#).

- Pour IMDSv2, vous devez utiliser **/latest/api/token** lors de la récupération du jeton.

L'envoi de requêtes PUT à tout chemin spécifique d'une version, par exemple `/2021-03-23/api/token`, a pour effet que le service de métadonnées retourne des erreurs 403 Interdit. Ce comportement est prévu.

- Si IMDSv2 est requis, IMDSv1 ne fonctionne pas.

Vous pouvez vérifier si IMDSv2 est requis pour une instance en procédant comme suit : sélectionnez l'instance pour en afficher les détails, puis vérifiez la valeur de IMDSv2. La valeur est soit Obligatoire (seul IMDSv2 peut être utilisé) ou Facultatif (IMDSv2 et IMDSv1 peuvent être utilisés).

Réponses et messages d'erreur

Toutes les métadonnées d'instance sont retournées sous forme de texte (type de contenu HTTP `text/plain`).

Une requête pour une ressource de métadonnées spécifique retourne la valeur appropriée ou un code d'erreur HTTP `404 - Not Found` si la ressource n'est pas disponible.

Une requête pour une ressource de métadonnées générale (l'URI se termine par un `/`) retourne une liste de ressources disponibles ou un code d'erreur HTTP `404 - Not Found` si une telle ressource n'existe pas. Les éléments de la liste se trouvent sur des lignes séparées se terminant par des sauts de ligne (ASCII 10).

Pour les demandes effectuées à l'aide d'Service des métadonnées d'instance Version 2, les codes d'erreur HTTP suivants peuvent être renvoyés :

- `400 - Missing or Invalid Parameters` – La demande PUT n'est pas valide.
- `401 - Unauthorized` – La demande GET utilise un jeton non valide. Il est recommandé dans ce cas de générer un nouveau jeton.
- `403 - Forbidden` : la demande n'est pas autorisée ou l'IMDS est désactivé.

Exemples de récupération des métadonnées d'instance

Les exemples suivants fournissent des commandes que vous pouvez utiliser sur une instance Amazon EC2. Le format de commande est différent pour les instances Linux et Windows.

Exemples

- [Obtenir les versions disponibles des métadonnées d'instance](#)
- [Obtenir les éléments de métadonnées de niveau supérieur](#)
- [Obtenir les valeurs des éléments de métadonnées](#)
- [Obtenir la liste des clés publiques disponibles](#)
- [Montrer les formats pour lesquels une clé publique 0 est disponible](#)
- [Obtenir la clé publique 0 \(au format clé OpenSSH\)](#)
- [Obtenir l'ID de sous-réseau d'une instance](#)
- [Obtenir les identifications d'une instance](#)

Obtenir les versions disponibles des métadonnées d'instance

Cet exemple permet d'obtenir les versions disponibles des métadonnées d'instance. Chaque version fait référence à un build de métadonnées d'instance lorsque de nouvelles catégories de métadonnées d'instance ont été publiées. Les versions de métadonnées d'instance ne sont pas en corrélation avec les versions de l'API Amazon EC2. Les versions antérieures sont disponibles au cas où vous ayez des scripts reposant sur la structure et les informations présentes dans une version précédente.

Note

Pour éviter de devoir mettre à jour votre code chaque fois qu'Amazon EC2 publie un nouveau build des métadonnées d'instance, nous vous recommandons d'utiliser `latest` dans le chemin d'accès, et non le numéro de version. Par exemple, utilisez `latest` comme suit :

```
curl http://169.254.169.254/latest/meta-data/ami-id
```

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/  
1.0  
2007-01-19  
2007-03-01  
2007-08-29  
2007-10-10  
2007-12-15  
2008-02-01  
2008-09-01  
2009-04-04  
2011-01-01  
2011-05-01  
2012-01-12  
2014-02-25  
2014-11-05  
2015-10-20  
2016-04-19  
...
```

```
latest
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/  
1.0  
2007-01-19  
2007-03-01  
2007-08-29  
2007-10-10  
2007-12-15  
2008-02-01  
2008-09-01  
2009-04-04  
2011-01-01  
2011-05-01  
2012-01-12  
2014-02-25  
2014-11-05  
2015-10-20  
2016-04-19  
...  
latest
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method  
GET -Uri http://169.254.169.254/  
1.0  
2007-01-19  
2007-03-01  
2007-08-29  
2007-10-10  
2007-12-15  
2008-02-01  
2008-09-01
```

```
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Obtenir les éléments de métadonnées de niveau supérieur

Cet exemple permet d'obtenir les éléments de métadonnées de niveau supérieur. Pour plus d'informations sur les éléments contenus dans la réponse, consultez [Catégories de métadonnées d'instance](#).

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
```

```
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
```

```
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

Obtenir les valeurs des éléments de métadonnées

Ces exemples obtiennent les valeurs de certains des éléments de métadonnées de niveau supérieur obtenus dans l'exemple précédent. Les demandes IMDSv2 utilisent le jeton stocké qui a été créé dans l'exemple de commande précédent, sous réserve qu'il ne soit pas arrivé à expiration.

Linux

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/  
latest/meta-data/ami-id  
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/  
latest/meta-data/reservation-id  
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/  
latest/meta-data/local-hostname  
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/  
latest/meta-data/public-hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id  
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id  
r-0efghijk987654321
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname  
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

Windows

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method  
GET -Uri http://169.254.169.254/latest/meta-data/ami-id  
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method  
GET -Uri http://169.254.169.254/latest/meta-data/reservation-id  
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method  
GET -Uri http://169.254.169.254/latest/meta-data/local-hostname  
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method  
GET -Uri http://169.254.169.254/latest/meta-data/public-hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id  
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-  
id  
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-  
hostname  
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-  
hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

Obtenir la liste des clés publiques disponibles

Cet exemple permet d'obtenir la liste des clés publiques disponibles.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/ 0=my-public-key
```

Montrer les formats pour lesquels une clé publique 0 est disponible

Cet exemple montre les formats pour lesquels une clé publique 0 est disponible.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Obtenir la clé publique 0 (au format clé OpenSSH)

Cet exemple permet d'obtenir la clé publique 0 (au format clé OpenSSH).

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCcAFICCCQD6m7oRw0uX0jANBgkqhkiG9w0BAQUFADCBiDELMAKGA1UEBhMCMC
VVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWw6
b24xFDASBgNVBAwTC01BTSBDb25zb2x1MRIwEAYDVQQDEw1UZXR0Q21sYWx1eHAd
BgkqhkiG9w0BCQEWEG5vb251QGftYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAKGA1UEBhMCMCVMxCzAJBgNVBAGTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWw6b24xFDASBgNVBAwTC01BTSBDb25z
b2x1MRIwEAYDVQQDEw1UZXR0Q21sYWx1eHAdBgkqhkiG9w0BCQEWEG5vb251QGft
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySwTC2XADZ4nB+BLygVIk60CpiwsZ3G93vUEI03IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITx0USQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnczvQAaRHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0Fkb
FFbjvSfpJI1J00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp3780D8uTs7fLvjx79LjStB
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCcAFICCCQD6m7oRw0uX0jANBgkqhkiG9w0BAQUFADCBiDELMAKGA1UEBhMCMC
VVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWw6
b24xFDASBgNVBAwTC01BTSBDb25zb2x1MRIwEAYDVQQDEw1UZXR0Q21sYWx1eHAd
BgkqhkiG9w0BCQEWEG5vb251QGftYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAKGA1UEBhMCMCVMxCzAJBgNVBAGTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWw6b24xFDASBgNVBAwTC01BTSBDb25z
b2x1MRIwEAYDVQQDEw1UZXR0Q21sYWx1eHAdBgkqhkiG9w0BCQEWEG5vb251QGft
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySwTC2XADZ4nB+BLygVIk60CpiwsZ3G93vUEI03IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITx0USQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnczvQAaRHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0Fkb
FFbjvSfpJI1J00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp3780D8uTs7fLvjx79LjStB
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCcAaFICCCQD6m7oRw0uX0jANBgkqhkiG9w0BAQUFADCBiDELMAKGA1UEBhMC
VVMxCzAJBgNVBAGTAldBMRAwDgYDVQQLhEwdGx1MQ8wDQYDVQKKEwZBbWF6
b24xFDASBgNVBAwTC01BTSBDb25zb2x1MRIwEAYDVQQDEwLUZXN0Q21sYWxhZAd
BgkqhkiG9w0BCQEWEG5vb251QGftYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAKGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYD
VQQLhEwdGx1MQ8wDQYDVQKKEwZBbWF6b24xFDASBgNVBAwTC01BTSBDb25z
b2x1MRIwEAYDVQQDEwLUZXN0Q21sYWxhZAdBgkqhkiG9w0BCQEWEG5vb251QGft
YXpvbi5jb20wZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLyGVIk60CpiwsZ3G93vUEI03IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITx0USQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnczvQAaRHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0Fkb
FFbjvSfpJIIJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp3780D8uTs7fLvjx79LjStB
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
ssh-rsa MIICiTCcAaFICCCQD6m7oRw0uX0jANBgkqhkiG9w0BAQUFADCBiDELMAKGA1UEBhMC
VVMxCzAJBgNVBAGTAldBMRAwDgYDVQQLhEwdGx1MQ8wDQYDVQKKEwZBbWF6
b24xFDASBgNVBAwTC01BTSBDb25zb2x1MRIwEAYDVQQDEwLUZXN0Q21sYWxhZAd
BgkqhkiG9w0BCQEWEG5vb251QGftYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAKGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYD
VQQLhEwdGx1MQ8wDQYDVQKKEwZBbWF6b24xFDASBgNVBAwTC01BTSBDb25z
b2x1MRIwEAYDVQQDEwLUZXN0Q21sYWxhZAdBgkqhkiG9w0BCQEWEG5vb251QGft
YXpvbi5jb20wZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLyGVIk60CpiwsZ3G93vUEI03IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITx0USQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnczvQAaRHhd1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0Fkb
FFbjvSfpJIIJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp3780D8uTs7fLvjx79LjStB
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Obtenir l'ID de sous-réseau d'une instance

Cet exemple permet d'obtenir l'ID de sous-réseau pour une instance.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Obtenir les identifications d'une instance

Dans les exemples suivants, l'exemple d'instance possède des [identifications sur les métadonnées d'instance activées](#) et les identifications d'instance Name=MyInstance et Environment=Dev.

Cet exemple permet d'obtenir toutes les clés d'identification d'une instance.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance
```

Name

Environment

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance
```

Name

Environment

L'exemple suivant montre la valeur de la clé Name obtenue dans l'exemple précédent. La demande IMDSv2 utilise le jeton stocké qui a été créé dans l'exemple de commande précédent, sous réserve qu'il ne soit pas arrivé à expiration.

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance/Name
```

MyInstance

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance/Name
```

MyInstance

Windows

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"  
= "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method  
GET -Uri http://169.254.169.254/latest/meta-data/tags/instance  
Name  
Environment
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/instance  
Name  
Environment
```

L'exemple suivant montre la valeur de la clé Name obtenue dans l'exemple précédent. La demande IMDSv2 utilise le jeton stocké qui a été créé dans l'exemple de commande précédent, sous réserve qu'il ne soit pas arrivé à expiration.

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method  
GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/Name  
MyInstance
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/  
instance/Name  
MyInstance
```

Limitation des demandes

Nous limitons les requêtes envoyées par chaque instance à l'IMDS et appliquons des limites au nombre de connexions simultanées possible depuis une instance vers l'IMDS.

Si vous utilisez l'IMDS pour récupérer des informations d'identification de AWS sécurité, évitez de demander des informations d'identification lors de chaque transaction ou simultanément à partir d'un grand nombre de threads ou de processus, car cela pourrait entraîner un ralentissement. Nous vous conseillons plutôt de placer les informations d'identification en cache jusqu'à ce que leur date d'expiration approche. Pour plus d'informations sur le rôle IAM et les informations d'identification de sécurité associées au rôle, consultez [Extraire les informations d'identification de sécurité à partir des métadonnées d'instance](#).

Si vous rencontrez des limitations alors que vous tentez d'accéder à l'IMDS, renvoyez une requête avec une stratégie de backoff exponentiel.

Limiter l'accès à l'IMDS

Vous pouvez envisager d'utiliser des règles de pare-feu locales pour désactiver l'accès à l'IMDS à partir de certains processus, voire tous.

Note

Pour les [instances basées sur le système AWS Nitro](#), l'IMDS est accessible depuis votre propre réseau lorsqu'un appareil réseau au sein de votre VPC, tel qu'un routeur virtuel, transmet des paquets à l'adresse IMDS et que le contrôle [source/destination](#) par défaut sur l'instance est désactivé. Pour empêcher une source extérieure à votre VPC d'atteindre l'IMDS, nous vous recommandons de modifier la configuration de l'appliance réseau afin de supprimer les paquets contenant l'adresse IPv4 de destination de l'IMDS 169.254.169.254 et, si vous avez activé le point de terminaison IPv6, l'adresse IPv6 de l'IMDS. [fd00:ec2::254]

Linux

Utilisation d'éléments iptables pour limiter l'accès

L'exemple suivant utilise des éléments Linux iptables et le module `owner` associé pour empêcher le serveur web Apache (en fonction de son ID utilisateur d'installation par défaut `apache`) d'accéder à l'adresse 169.254.169.254. Il utilise une règle `deny` pour rejeter toutes les demandes de métadonnées d'instance (IMDSv1 ou IMDSv2) de tout processus s'exécutant au nom de cet utilisateur.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner --uid-owner apache --jump REJECT
```

Vous pouvez aussi envisager d'autoriser uniquement l'accès à des utilisateurs ou des groupes particuliers à l'aide de règles d'autorisation (allow). Les règles allow peuvent être plus faciles à gérer du point de vue de la sécurité, car elles nécessitent que vous déterminiez quels sont les logiciels ayant besoin d'accéder aux métadonnées d'instance. Si vous utilisez des règles allow, vous risquez moins d'autoriser accidentellement un logiciel à accéder au service des métadonnées en cas de modification ultérieure des logiciels ou de la configuration sur une instance. Vous pouvez également combiner une utilisation de groupes avec des règles allow, afin de pouvoir ajouter et supprimer des utilisateurs dans un groupe autorisé sans avoir à modifier la règle du pare-feu.

L'exemple suivant empêche tous les processus d'accéder à l'IMDS, à l'exception des processus qui s'exécutent dans le compte utilisateur `trustworthy-user`.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner ! --uid-owner trustworthy-user --jump REJECT
```

Note

- Pour utiliser des règles de pare-feu locales, vous devez adapter les commandes de l'exemple précédent à vos besoins.
- Par défaut, les règles iptables ne sont pas persistantes après un redémarrage du système. Elles peuvent être rendues persistantes en utilisant des fonctionnalités du système d'exploitation qui ne sont pas décrites ici.
- Le module iptables `owner` correspond uniquement à l'appartenance au groupe si le groupe est le groupe principal d'un utilisateur local donné. Les autres groupes n'ont pas de correspondance.

Utilisation de PF ou de IPFW pour limiter l'accès

Si vous utilisez FreeBSD ou OpenBSD, vous pouvez également envisager d'utiliser PF ou IPFW. Les exemples suivants permettent de limiter l'accès à l'IMDS à l'utilisateur root uniquement.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

Note

L'ordre des commandes PF et IPFW a de l'importance. PF prend par défaut la valeur de la dernière règle correspondante et IPFW prend par défaut la valeur de la première règle correspondante.

Windows

Utilisation du pare-feu Windows pour limiter l'accès

L' PowerShell exemple suivant utilise le pare-feu Windows intégré pour empêcher le serveur Web Internet Information Server (sur la base de son ID utilisateur d'installation par défaut NT AUTHORITY \IUSR) d'accéder au 169.254.169.254. Il utilise une règle deny pour rejeter toutes les demandes de métadonnées d'instance (IMDSv1 ou IMDSv2) de tout processus s'exécutant au nom de cet utilisateur.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT  
AUTHORITY\IUSR")  
PS C:\> $BlockPrincipalSID =  
$blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value  
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"  
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action  
block -Direction out `  
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

Vous pouvez aussi envisager d'autoriser uniquement l'accès à des utilisateurs ou des groupes particuliers à l'aide de règles d'autorisation (allow). Les règles allow peuvent être plus faciles à gérer du point de vue de la sécurité, car elles nécessitent que vous déterminiez quels sont les logiciels

ayant besoin d'accéder aux métadonnées d'instance. Si vous utilisez des règles allow, vous risquez moins d'autoriser accidentellement un logiciel à accéder au service des métadonnées en cas de modification ultérieure des logiciels ou de la configuration sur une instance. Vous pouvez également combiner une utilisation de groupes avec des règles allow, afin de pouvoir ajouter et supprimer des utilisateurs dans un groupe autorisé sans avoir à modifier la règle du pare-feu.

L'exemple suivant empêche tous les processus s'exécutant en tant que groupe OS spécifié dans la variable `blockPrincipal` (dans cet exemple, le groupe Windows Everyone) d'accéder aux métadonnées d'instance, à l'exception des processus spécifiés dans `exceptionPrincipal` (dans cet exemple, un groupe appelé `trustworthy-users`). Vous devez spécifier à la fois des principaux d'autorisation (allow) et de refus (deny), car le pare-feu Windows, contrairement à la règle `--uid-owner trustworthy-user` dans les éléments Linux iptables, ne fournit pas de mécanisme de raccourci permettant d'autoriser uniquement un principal particulier (utilisateur ou groupe) en refusant l'accès à tous les autres.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
("Everyone")
PS C:\> $BlockPrincipalSID =
  $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
  $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;;CC;;;$ExceptionPrincipalSID)(A;;;CC;;;
$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
  $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
  Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

Note

Pour utiliser des règles de pare-feu locales, vous devez adapter les commandes de l'exemple précédent à vos besoins.

Utilisation de règles netsh pour limiter l'accès

Vous pouvez envisager de bloquer tous les logiciels à l'aide de règles netsh, mais ces règles sont beaucoup moins souples.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"  
dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

Note

- Pour utiliser des règles de pare-feu locales, vous devez adapter les commandes de l'exemple précédent à vos besoins.
- netsh Les règles doivent être définies à partir d'une invite de commande élevée et ne peuvent pas être définies sur des principaux deny ou allow particuliers.

Utiliser les données utilisateur d'instance

Vous pouvez utiliser les données utilisateur d'instance pour personnaliser vos instances. Lorsque vous lancez une instance, vous pouvez stocker des paramètres ou des scripts sous forme de données utilisateur. Tous les scripts des données utilisateur sont exécutés lorsque vous lancez l'instance. Vous pouvez afficher les données utilisateur sous forme d'attribut d'instance. Vous pouvez également afficher les données utilisateur de votre instance via le service de métadonnées d'instance (IMDS).

Considérations

- Les données utilisateur sont traitées comme des données opaques : ce que vous donnez est ce que vous obtenez en retour. Il appartient à l'instance de l'interpréter.
- Les données utilisateur doivent être codées en base64. La console Amazon EC2 peut effectuer l'encodage base64 pour vous ou accepter les entrées codées en base64.
- Les données d'utilisateur sont limitées à 16 Ko en format brut, avant qu'elles soient encodées en base64. La taille d'une chaîne de longueur n après l'encodage base64 est $\text{ceil}(n/3)*4$.
- Les données utilisateur doivent être décodées en base64 lorsque vous les récupérez. Si vous les récupérez à l'aide des métadonnées d'instance ou de la console, les données sont décodées automatiquement.
- Si vous arrêtez une instance, modifiez ses données utilisateur et démarrez l'instance, les données utilisateur mises à jour ne sont pas exécutées automatiquement lorsque vous démarrez l'instance. Avec les instances Windows, vous pouvez configurer les paramètres de manière à ce que les scripts de données utilisateur mis à jour soient exécutés une fois lorsque vous démarrez l'instance ou chaque fois que vous redémarrez ou démarrez l'instance.

- Les données utilisateur sont un attribut d'instance. Si vous créez une AMI à partir d'une instance, les données utilisateur d'instance ne sont pas incluses dans l'AMI.

Spécification des données utilisateur d'instance au moment du lancement

Vous pouvez spécifier des données utilisateur lorsque vous lancez une instance. Pour obtenir des instructions de la console, consultez [Spécification des données utilisateur d'instance au moment du lancement](#). Pour un exemple de Linux utilisant le AWS CLI, voir [the section called "Les données utilisateur et le AWS CLI"](#). Pour un exemple de Windows utilisant les outils pour Windows PowerShell, voir [the section called "Les données utilisateur et les outils pour Windows PowerShell"](#).

Modification des données utilisateur d'instance

Vous pouvez modifier les données utilisateur pour les instances dotées d'un volume racine EBS. L'instance doit être à l'état arrêté. Pour obtenir des instructions de la console, consultez [Affichage et mise à jour des données utilisateur d'instance](#). Pour un exemple de Linux utilisant le AWS CLI, voir [modify-instance-attribute](#). Pour un exemple de Windows utilisant les outils pour Windows PowerShell, voir [the section called "Les données utilisateur et les outils pour Windows PowerShell"](#).

Récupération des données utilisateur d'instance depuis votre instance

Note

Les exemples de cette section utilisent l'adresse IPv4 de l'IMDS : 169.254.169.254. Si vous récupérez des métadonnées d'instance pour les instances EC2 sur l'adresse IPv6, assurez-vous d'activer et d'utiliser l'adresse IPv6 à la place : [fd00:ec2::254]. L'adresse IPv6 de l'IMDS est compatible avec les commandes IMDSv2. L'adresse IPv6 n'est accessible que sur [les instances créées sur le système AWS Nitro](#) et dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement).

Pour récupérer des données utilisateur depuis une instance, utilisez l'URI ci-après.

```
http://169.254.169.254/latest/user-data
```

Une demande de données utilisateur renvoie les données telles qu'elles sont (type de contenu `application/octet-stream`). Si l'instance ne possède aucune donnée utilisateur, la demande renvoie `404 - Not Found`.

Cet exemple renvoie les données utilisateur qui ont été fournies sous la forme de texte séparé par des virgules.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri
http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Cet exemple renvoie des données utilisateur qui ont été fournies sous la forme d'un script.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>>true</persist>
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
```

```
New-Item $file -ItemType file
</powershell>
<persist>>true</persist>
```

Récupération des données utilisateur d'instance depuis votre ordinateur

Vous pouvez récupérer des données utilisateur pour une instance à partir de votre ordinateur. Pour obtenir des instructions de la console, consultez [Affichage et mise à jour des données utilisateur d'instance](#). Pour un exemple utilisant le AWS CLI, voir [Les données utilisateur et le AWS CLI](#). Pour un exemple utilisant les outils pour Windows PowerShell, voir [Les données utilisateur et les outils pour Windows PowerShell](#).

Récupérer des données dynamiques

Pour récupérer des données dynamiques depuis une instance en cours d'exécution, utilisez l'URI ci-après.

```
http://169.254.169.254/latest/dynamic/
```

Note

Les exemples de cette section utilisent l'adresse IPv4 de l'IMDS : 169.254.169.254. Si vous récupérez des métadonnées d'instance pour les instances EC2 sur l'adresse IPv6, assurez-vous d'activer et d'utiliser l'adresse IPv6 à la place : [fd00:ec2::254]. L'adresse IPv6 de l'IMDS est compatible avec les commandes IMDSv2. L'adresse IPv6 n'est accessible que sur [les instances créées sur le système AWS Nitro](#) et dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement).

Cet exemple montre comment récupérer les catégories d'identité d'instance de haut niveau.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/
```

```
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

Pour plus d'informations sur les données dynamiques et pour des exemples sur la façon de les récupérer, consultez [Documents d'identité d'instance](#).

Catégories de métadonnées d'instance

Les métadonnées d'instance sont divisées en plusieurs catégories. Pour récupérer les métadonnées d'instance, vous spécifiez la catégorie dans la demande et les métadonnées sont renvoyées dans la réponse.

Lorsque de nouvelles catégories sont publiées, un nouveau build de métadonnées d'instance est créé avec un nouveau numéro de version. Dans le tableau suivant, la colonne Version when category was released (Version lors de la publication de la catégorie) indique la version du build lorsqu'une catégorie de métadonnées d'instance a été publiée. Pour éviter de devoir mettre à jour votre code chaque fois qu'Amazon EC2 publie une nouvelle version de métadonnées d'instance, utilisez `latest` au lieu du numéro de version dans vos demandes de métadonnées. Pour plus d'informations, consultez [Obtenir les versions disponibles des métadonnées d'instance](#).

Lorsque Amazon EC2 libère une nouvelle catégorie de métadonnées d'instance, les métadonnées d'instance de la nouvelle catégorie peuvent ne pas être disponibles pour les instances existantes. Avec une instance basée sur le [système Nitro](#), vous ne pouvez récupérer les métadonnées de l'instance que pour les catégories qui étaient disponibles au lancement. Pour une instance avec l'hyperviseur Xen, vous pouvez [l'arrêter puis la démarrer](#) afin de mettre à jour les catégories disponibles pour cette instance.

Le tableau ci-après répertorie les catégories de métadonnées d'instance. Certains noms de catégorie incluent des espaces réservés pour les données, qui sont propres à votre instance. Par exemple, `mac` représente l'adresse MAC de l'interface réseau. Quand vous récupérez les métadonnées de l'instance, vous devez remplacer les espaces réservés par des valeurs réelles.

Catégorie	Description	Version lors de la publication de la catégorie
<code>ami-id</code>	L'ID d'AMI utilisé pour lancer l'instance.	1.0
<code>ami-launch-index</code>	Si vous lancez plusieurs instances à l'aide du même <code>RunInstances</code> appel, cette valeur indique l'ordre de lancement de chaque instance. La valeur 0 indique la première	1.0

Catégorie	Description	Version lors de la publication de la catégorie
	instance lancée. Si vous lancez des instances à l'aide d'Auto Scaling ou d'un parc EC2, cette valeur est toujours égale à 0.	
<code>ami-manifest-path</code>	Chemin d'accès du fichier manifeste d'AMI dans Amazon S3. Si vous avez utilisé une AMI basée sur Amazon EBS pour lancer l'instance, le résultat retourné est <code>unknown</code> .	1.0
<code>ancestor-ami-ids</code>	Les ID d'AMI de toutes les instances qui ont été regroupées pour créer cette AMI. Cette valeur n'existera que si le fichier manifeste d'AMI contenait une clé <code>ancestor-amis</code> .	2007-10-10

Catégorie	Description	Version lors de la publication de la catégorie
autoscaling/target-lifecycle-state	Valeur indiquant l'état cible du cycle de vie Auto Scaling vers lequel une instance Auto Scaling est en train de passer. Présent lorsque l'instance passe à l'un des états de cycle de vie cibles après le 10 mars 2022. Valeurs possibles : Detached InService Standby Terminated Warmed:Hibernated Warmed:Running Warmed:Stopped Warmed:Terminated . Consultez Récupérer l'état du cycle de vie cible par le biais des métadonnées d'instance dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.	15/07/2021
block-device-mapping/ami	Le périphérique virtuel qui contient le système de fichiers racine/démarrage.	2007-12-15
block-device-mapping/ebs N	Les périphériques virtuels associés à tout volume Amazon EBS. Les volumes Amazon EBS ne sont disponibles dans les métadonnées que s'ils étaient présents au moment du lancement ou lorsque l'instance a été démarrée pour la dernière fois. Le N indique l'index du volume Amazon EBS (tel que ebs1 ou ebs2).	2007-12-15

Catégorie	Description	Version lors de la publication de la catégorie
block-device-mapping/ephemeralN	Les appareils virtuels pour les volumes de stockage d'instances non NVMe. Le N indique l'index de chaque volume. Le nombre de volumes de stockage d'instances dans le mappage d'appareils en bloc peut ne pas correspondre au nombre réel de volumes de stockage d'instances pour l'instance. Le type d'instance détermine le nombre de volumes de stockage d'instances disponibles pour une instance. Si le nombre de volumes de stockage d'instances dans un mappage d'appareils en bloc dépasse le nombre disponible pour une instance, les volumes de stockage d'instances supplémentaires sont ignorés.	2007-12-15
block-device-mapping/root	Les périphériques ou partitions virtuels associés aux périphériques ou partitions racines sur le périphérique virtuel où le système de fichiers racine (/ ou C:) est associé avec l'instance donnée.	2007-12-15
block-device-mapping/swap	Les périphériques virtuels associés avec swap. Pas toujours présents.	2007-12-15

Catégorie	Description	Version lors de la publication de la catégorie
<code>elastic-gpus/associations/ <i>elastic-gpu-id</i></code>	Si un Elastic GPU est attaché à l'instance, contient une chaîne JSON avec des informations sur l'Elastic GPU, notamment son ID et ses informations de connexion.	2016-11-30
<code>elastic-inference/associations/ <i>eia-id</i></code>	Si un accélérateur Elastic Inference est attaché à l'instance, contient une chaîne JSON avec des informations sur l'accélérateur Elastic Inference, notamment son ID et son type.	2018-11-29
<code>events/maintenance/history</code>	S'il y a des événements de maintenance terminés ou annulés pour l'instance, contient une chaîne JSON avec des informations sur ces événements. Pour plus d'informations, consultez Pour afficher l'historique des événements terminés ou annulés .	2018-08-17
<code>events/maintenance/scheduled</code>	S'il y a des événements de maintenance activés pour l'instance, contient une chaîne JSON avec des informations sur ces événements. Pour plus d'informations, consultez Afficher les événements planifiés .	2018-08-17

Catégorie	Description	Version lors de la publication de la catégorie
events/recommendations/rebalance	<p>Heure approximative, UTC, à laquelle la notification de recommandation de rééquilibrage d'instance EC2 est émise pour l'instance. Voici un exemple de métadonnées pour cette catégorie : {"noticeTime": "2020-11-05T08:22:00Z"}</p> <p>. Cette catégorie n'est disponible qu'après l'émission de la notification. Pour plus d'informations, consultez Recommandations de rééquilibrage des instances EC2.</p>	27/10/2020
hostname	<p>Si l'instance EC2 utilise l'appellation basée sur l'adresse IP (IPBN), il s'agit du nom d'hôte DNS IPv4 privé de l'instance. Si l'instance EC2 utilise l'appellation basée sur les ressources (RBN), il s'agit du RBN. Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique eth0 (le périphérique dont le numéro de périphérique est 0). Pour plus d'informations sur IPBN et RBN, consultez Types de noms d'hôtes des instances Amazon EC2.</p>	1.0

Catégorie	Description	Version lors de la publication de la catégorie
iam/info	Si un rôle IAM est associé à l'instance, il contient des informations sur la dernière mise à jour du profil de l'instance, notamment la LastUpdated date et l'InstanceProfileidentifiant de l'instance. InstanceProfileArn Sinon, absent.	2012-01-12
iam/security-credentials/role-name	Si un rôle IAM est associé à l'instance, <i>nom-rôle</i> est le nom du rôle et <i>nom-rôle</i> contient les informations d'identification de sécurité temporaires associées au rôle (pour plus d'informations, consultez Extraire les informations d'identification de sécurité à partir des métadonnées d'instance). Sinon, absent.	2012-01-12
identity-credentials/ec2/info	Informations sur les informations d'identification dans identity-credentials/ec2/security-credentials/ec2-instance .	2018-05-23

Catégorie	Description	Version lors de la publication de la catégorie
<code>identity-credentials/ec2/security-credentials/ec2-instance</code>	Informations d'identification pour le rôle d'identité d'instance qui permettent au logiciel sur instance de s'identifier afin de AWS prendre en charge des fonctionnalités telles que EC2 Instance Connect et la configuration de gestion d'hôte AWS Systems Manager par défaut. Ces informations d'identification ne sont associées à aucune politique, elles ne disposent donc d'aucune autorisation d' AWS API supplémentaire autre que l'identification de l'instance par rapport à la AWS fonctionnalité. Pour plus d'informations, consultez Rôles d'identité d'instance .	2018-05-23
<code>instance-action</code>	Informe l'instance qu'elle devrait redémarrer en vue de la création d'un bundle. Valeurs valides : <code>none</code> <code>shutdown</code> <code>bundle-pending</code> .	2008-09-01
<code>instance-id</code>	L'ID de cette instance.	1.0
<code>instance-life-cycle</code>	Option d'achat de cette instance. Pour plus d'informations, consultez Options d'achat d'instance .	01-10-2019
<code>instance-type</code>	Le type d'instance. Pour plus d'informations, consultez Types d'instances Amazon EC2 .	2007-08-29

Catégorie	Description	Version lors de la publication de la catégorie
ipv6	L'adresse IPv6 de l'instance. Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence à l'interface réseau du périphérique eth0 (le périphérique dont le numéro de périphérique est 0) et à la première adresse IPv6 attribuée. Si aucune adresse IPv6 n'existe sur l'interface réseau [0], cet élément n'est pas défini et génère une réponse HTTP 404.	03/01/2021
kernel-id	L'ID du noyau lancé avec l'instance, le cas échéant.	2008-02-01
local-hostname	Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique eth0 (le périphérique dont le numéro de périphérique est 0). Si l'instance EC2 utilise l'appellation basée sur l'adresse IP (IPBN), il s'agit du nom d'hôte DNS IPv4 privé de l'instance. Si l'instance EC2 utilise l'appellation basée sur les ressources (RBN), il s'agit du RBN. Pour plus d'informations sur IPBN, RBN et l'appellation des instances EC2, consultez Types de noms d'hôtes des instances Amazon EC2 .	2007-01-19

Catégorie	Description	Version lors de la publication de la catégorie
<code>local-ipv4</code>	L'adresse IPv4 privée de l'instance. Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique <code>eth0</code> (le périphérique dont le numéro de périphérique est 0). S'il s'agit d'une instance IPv6 uniquement, cet élément n'est pas défini et génère une réponse HTTP 404.	1.0
<code>mac</code>	L'adresse de contrôle d'accès média (MAC) de l'instance. Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique <code>eth0</code> (le périphérique dont le numéro de périphérique est 0).	2011-01-01
<code>metrics/vhostmd</code>	Plus disponible.	2011-05-01
<code>network/interfaces/macs/mac/device-number</code>	Le numéro de périphérique unique associé à cette interface. Le numéro de périphérique correspond au nom du périphérique, par exemple un <code>device-number</code> de 2 est pour le périphérique <code>eth2</code> . Cette catégorie correspond aux champs <code>DeviceIndex</code> et <code>device-index</code> utilisés par l'API Amazon EC2 et les commandes EC2 pour la AWS CLI.	2011-01-01

Catégorie	Description	Version lors de la publication de la catégorie
network/interfaces/macs/mac/interface-id	L'ID de l'interface réseau.	2011-01-01
network/interfaces/macs/mac/ipv4-associations/public-ip	Les adresses IPv4 privées qui sont associées à chaque adresse IP publique et assignées à cette interface.	2011-01-01
network/interfaces/macs/mac/ipv6s	Les adresses IPv6 attribuées à l'interface.	2016-06-30
network/interfaces/macs/mac/ipv6-prefix	Le préfixe IPv6 attribué à l'interface réseau.	
network/interfaces/macs/mac/local-hostname	Le nom d'hôte DNS IPv4 privé de l'instance. Dans le cas où plusieurs interfaces réseau sont présentes, cela fait référence au périphérique eth0 (le périphérique dont le numéro de périphérique est 0). S'il s'agit d'une instance IPv6 uniquement, il s'agit du nom basé sur les ressources. Pour plus d'informations sur IPBN et RBN, consultez Types de noms d'hôtes des instances Amazon EC2 .	2007-01-19
network/interfaces/macs/mac/local-ipv4s	Les adresses IPv4 privées associées à l'interface. S'il s'agit d'une interface réseau IPv6 uniquement, cet élément n'est pas défini et génère une réponse HTTP 404.	2011-01-01

Catégorie	Description	Version lors de la publication de la catégorie
network/interfaces/macs/mac/mac	L'adresse MAC de l'instance.	2011-01-01
network/interfaces/macs/ <i>mac</i> /network-card	L'index de la carte réseau. Certains types d'instance prennent en charge plusieurs cartes réseau.	2020-11-01
network/interfaces/macs/mac/owner-id	L'ID du propriétaire de l'interface réseau. Dans les environnements à interfaces multiples, une interface peut être attachée à un tiers, par exemple Elastic Load Balancing. Le trafic sur l'interface est toujours facturé au propriétaire de l'interface.	2011-01-01
network/interfaces/macs/mac/public-hostname	Le DNS public de l'interface (IPv4). Cette catégorie n'est retournée que si l'attribut <code>enableDnsHostnames</code> est défini comme <code>true</code> . Pour plus d'informations, consultez DNS attributes for your VPC (Attributs DNS pour votre VPC) dans le Guide de l'utilisateur d'Amazon VPC. Si l'instance ne possède qu'une adresse IPv6 publique et aucune adresse IPv4 publique, cet élément n'est pas défini et génère une réponse HTTP 404.	2011-01-01

Catégorie	Description	Version lors de la publication de la catégorie
<code>network/interfaces/macs/mac/public-ipv4s</code>	L'adresse IP publique ou les adresses IP Elastic associées à l'interface. Il peut y avoir plusieurs adresses IPv4 sur une instance.	2011-01-01
<code>network/interfaces/macs/mac/security-groups</code>	Les groupes de sécurité auxquels l'interface réseau appartient.	2011-01-01
<code>network/interfaces/macs/mac/security-group-ids</code>	Les ID des groupes de sécurité auxquels l'interface réseau appartient.	2011-01-01
<code>network/interfaces/macs/mac/subnet-id</code>	L'ID du sous-réseau (subnet) dans lequel l'interface réside.	2011-01-01
<code>network/interfaces/macs/mac/subnet-ipv4-cidr-block</code>	Le bloc d'adresse CIDR IPv4 du sous-réseau dans lequel l'interface réside.	2011-01-01
<code>network/interfaces/macs/mac/subnet-ipv6-cidr-blocks</code>	Le bloc d'adresse CIDR IPv6 du sous-réseau dans lequel l'interface réside.	2016-06-30
<code>network/interfaces/macs/mac/vpc-id</code>	L'ID du VPC dans lequel l'interface réside.	2011-01-01
<code>network/interfaces/macs/mac/vpc-ipv4-cidr-block</code>	Le bloc d'adresse CIDR IPv4 principal pour le VPC.	2011-01-01
<code>network/interfaces/macs/mac/vpc-ipv4-cidr-blocks</code>	Les blocs d'adresse CIDR IPv4 pour le VPC.	2016-06-30

Catégorie	Description	Version lors de la publication de la catégorie
network/interfaces/mac/mac/vpc-ipv6-cidr-blocks	Le bloc d'adresse CIDR IPv6 du VPC dans lequel l'interface réside.	2016-06-30
placement/availability-zone	La zone de disponibilité dans laquelle l'instance a été lancée.	2008-02-01
placement/availability-zone-id	ID de zone de disponibilité statique dans laquelle l'instance est lancée. L'ID de zone de disponibilité est cohérent entre les comptes. Toutefois, il peut être différent de la zone de disponibilité, qui peut varier selon le compte.	01-10-2019
placement/group-name	Nom du groupe de placement dans lequel l'instance est lancée.	2020-08-24
placement/host-id	ID de l'hôte sur lequel l'instance est lancée. Applicable uniquement aux Hôtes dédiés.	2020-08-24
placement/partition-number	Numéro de la partition dans laquelle l'instance est lancée.	2020-08-24
placement/region	AWS Région dans laquelle l'instance est lancée.	2020-08-24
product-codes	AWS Marketplace les codes de produit associés à l'instance, le cas échéant.	2007-03-01

Catégorie	Description	Version lors de la publication de la catégorie
<code>public-hostname</code>	Le DNS public de l'instance (IPv4). Cette catégorie n'est retournée que si l'attribut <code>enableDnsHostnames</code> est défini comme <code>true</code> . Pour plus d'informations, consultez DNS attributes for your VPC (Attributs DNS pour votre VPC) dans le Guide de l'utilisateur d'Amazon VPC. Si l'instance ne possède qu'une adresse IPv6 publique et aucune adresse IPv4 publique, cet élément n'est pas défini et génère une réponse HTTP 404.	2007-01-19
<code>public-ipv4</code>	L'adresse IPv4 publique. Si une adresse IP Elastic est associée à l'instance, la valeur retournée est l'adresse IP Elastic.	2007-01-19
<code>public-keys/0/openssh-key</code>	Clé publique. Disponible uniquement si fournie au moment du lancement de l'instance.	1.0
<code>ramdisk-id</code>	L'ID du disque RAM spécifié au moment du lancement, le cas échéant.	2007-10-10
<code>reservation-id</code>	L'ID de la réservation.	1.0

Catégorie	Description	Version lors de la publication de la catégorie
security-groups	<p>Les noms des groupes de sécurité appliqués à l'instance.</p> <p>Après le lancement, vous pouvez modifier les groupes de sécurité des instances. De tels changements apparaissent ici et dans réseau/interfaces/macs/<i>mac</i>/groupes-sécurité.</p>	1.0
services/domain	Le domaine des AWS ressources pour la région.	2014-02-25
services/partition	Partition dans laquelle se trouve la ressource. Pour les AWS régions standard, la partition est <code>aws</code> . Si vous avez des ressources dans d'autres partitions, la partition est <code>aws-<i>partitionname</i></code> . Par exemple, la partition des ressources de la région Chine (Beijing) est <code>aws-cn</code> .	2015-10-20
spot/instance-action	L'action (hibernation, arrêt ou résiliation) et l'heure approximative (UTC) à laquelle l'action aura lieu. Cet élément est présent uniquement si l'instance Spot a été balisée pour être mise en veille prolongée, arrêtée ou résiliée. Pour plus d'informations, consultez instance-action .	2016-11-15

Catégorie	Description	Version lors de la publication de la catégorie
spot/termination-time	L'heure approximative (indiquée au format UTC) à laquelle le système d'exploitation de votre instance Spot recevra le signal d'arrêt. Cet élément n'est présent et ne contient une valeur temporelle (par exemple, 2015-01-05T18:02:00Z) que si l'instance Spot a été balisée en vue de son arrêt par Amazon EC2. L'élément heure-arrêt n'est pas défini à une heure précise si vous avez mis fin vous-même à l'instance Spot. Pour plus d'informations, consultez termination-time .	2014-11-05
tags/instance	Identifications associées à l'instance. Disponible uniquement si vous autorisez explicitement l'accès aux identifications dans les métadonnées d'instance. Pour plus d'informations, consultez Autoriser l'accès aux identifications dans les métadonnées d'instance .	23/03/2021

Catégories de données dynamiques

Le tableau ci-après répertorie les catégories de données dynamiques.

Catégorie	Description	Version lors de la publication de la catégorie
fws/instance-monitoring	Valeur indiquant si le client a activé le suivi détaillé d'une minute dans CloudWatch. Valeurs valides : enabled disabled	2009-04-04
instance-identity/document	JSON contenant les attributs d'instance, tels que l'ID d'instance, l'adresse IP privée, etc. veuillez consulter Documents d'identité d'instance .	2009-04-04
instance-identity/pkcs7	Utilisé pour vérifier l'authenticité et le contenu du document par rapport à la signature. veuillez consulter Documents d'identité d'instance .	2009-04-04
instance-identity/signature	Les données pouvant être utilisées par d'autres pour vérifier leur origine et leur authenticité. veuillez consulter Documents d'identité d'instance .	2009-04-04

Exemple Linux : valeur de l'index de lancement de l'AMI

Cet exemple montre comment vous pouvez utiliser à la fois les données utilisateur et les métadonnées d'instance pour configurer vos instances Linux.

Note

Les exemples de cette section utilisent l'adresse IPv4 de l'IMDS : 169.254.169.254. Si vous récupérez des métadonnées d'instance pour les instances EC2 sur l'adresse IPv6, assurez-vous d'activer et d'utiliser l'adresse IPv6 à la place : [fd00:ec2::254]. L'adresse IPv6 de l'IMDS est compatible avec les commandes IMDSv2. L'adresse IPv6 n'est accessible que sur [les instances créées sur le système AWS Nitro](#) et dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement).

Alice souhaite lancer quatre instances de son AMI de base de données préférée ; la première instance servant d'instance initiale et les trois autres de réplicas. Lorsqu'elle les lance, elle souhaite ajouter des données utilisateur portant sur la stratégie de réplication pour chaque réplica. Elle sait que ces données seront disponibles pour les quatre instances. Elle a donc besoin de structurer les données utilisateur de sorte que chaque instance reconnaisse quelles parties la concernent. Pour ce faire, elle peut utiliser la valeur de métadonnées d'instance `ami-launch-index` qui sera unique pour chaque instance. Si elle démarre plus d'une instance à la fois, la valeur `ami-launch-index` indique l'ordre dans lequel les instances ont été lancées. La valeur de la première instance lancée est `0`.

Voici les données utilisateur construites par Alice.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

La donnée `replicate-every=1min` définit la configuration du premier réplica, `replicate-every=5min` définit la configuration du deuxième réplica, et ainsi de suite. Alice décide de fournir ces données sous la forme d'une chaîne ASCII avec un symbole barre verticale (|) délimitant les données pour les différentes instances.

Alice lance quatre instances à l'aide de la commande [run-instances](#), en spécifiant les données utilisateur.

```
aws ec2 run-instances \  
  --image-id ami-0abcdef1234567890 \  
  --count 4 \  
  --instance-type t2.micro \  
  --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Après leur lancement, toutes les instances ont une copie des données utilisateur et des métadonnées communes présentées ici :

- ID d'AMI : `ami-0abcdef1234567890`
- ID de réservation : `r-1234567890abcabc0`
- Clés publiques : aucune
- Nom du groupe de sécurité : par défaut
- Type d'instance : `t2.micro`

Toutefois, chaque instance possède certaines métadonnées uniques.

Instance 1

Metadonnées	Valeur
instance-id	i-1234567890abcdef0
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

Instance 2

Metadonnées	Valeur
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

Instance 3

Metadonnées	Valeur
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com

Metadonnées	Valeur
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

Instance 4

Metadonnées	Valeur
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice peut utiliser la valeur `ami-launch-index` pour déterminer quelle portion des données utilisateur est applicable à une instance particulière.

1. Elle se connecte à l'une des instances et récupère `ami-launch-index` pour cette instance afin de s'assurer qu'il s'agit de l'un des réplicas :

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-launch-index  
2
```

Pour les étapes suivantes, les demandes IMDSv2 utilisent le jeton stocké provenant de la commande IMDSv2 précédente, à condition que le jeton ne soit pas arrivé à expiration.

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index  
2
```

2. Elle enregistre les données `ami-launch-index` sous forme de variable.

IMDSv2

```
[ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"  
http://169.254.169.254/latest/meta-data/ami-launch-index`
```

IMDSv1

```
[ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-  
launch-index`
```

3. Elle enregistre les données utilisateur sous forme de variable.

IMDSv2

```
[ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN"  
http://169.254.169.254/latest/user-data`
```

IMDSv1

```
[ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
```

4. Enfin, Alice utilise la commande `cut` pour extraire la portion de données utilisateur applicable à cette instance.

IMDSv2

```
[ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"  
replicate-every=5min
```

IMDSv1

```
[ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"  
replicate-every=5min
```

Documents d'identité d'instance

Chaque instance que vous lancez a un Documents d'identité d'instance qui fournit des informations sur l'instance elle-même. Vous pouvez utiliser le Documents d'identité d'instance pour valider les attributs de l'instance.

Le document d'identité d'instance est généré lorsque l'instance est arrêtée et démarrée, redémarrée ou lancée. Le document d'identité d'instance est exposé (au format JSON en texte brut) via le service des métadonnées d'instance (IMDS). L'adresse IPv4 169.254.169.254 est une adresse de lien local et est uniquement valable à partir de l'instance. Pour plus d'informations, consultez [Link-local address](#) sur Wikipedia. L'adresse IPv6 [fd00:ec2::254] est une adresse de lien local et est uniquement valable à partir de l'instance. Pour plus d'informations, consultez [Unique local address](#) (adresse locale unique) sur Wikipedia.

Note

Les exemples de cette section utilisent l'adresse IPv4 de l'IMDS : 169.254.169.254. Si vous récupérez des métadonnées d'instance pour les instances EC2 sur l'adresse IPv6, assurez-vous d'activer et d'utiliser l'adresse IPv6 à la place : [fd00:ec2::254]. L'adresse IPv6 de l'IMDS est compatible avec les commandes IMDSv2. L'adresse IPv6 n'est accessible que sur [les instances créées sur le système AWS Nitro](#) et dans un [sous-réseau compatible IPv6](#) (double pile ou IPv6 uniquement).

Vous pouvez récupérer le Documents d'identité d'instance à partir d'une instance en cours d'exécution à tout moment. Le Documents d'identité d'instance contient les informations suivantes :

non structurées	Description
accountId	L'ID du AWS compte qui a lancé l'instance.
architecture	Architecture de l'AMI utilisée pour lancer l'instance (i386 x86_64 arm64).
availabilityZone	Zone de disponibilité dans laquelle l'instance est en cours d'exécution.
billingProducts	Produits de facturation de l'instance.

non structurées	Description
devpayPro ductCodes	Obsolète.
imageId	ID de l'AMI utilisée pour lancer l'instance.
instanceId	ID de l'instance.
instanceType	Type de l'instance.
kernelId	ID du noyau associé à l'instance, le cas échéant.
marketpla ceProductCodes	Le code AWS Marketplace produit de l'AMI utilisé pour lancer l'instance.
pendingTime	Date et heure auxquelles l'instance a été lancée.
privateIp	L'adresse IPv4 privée de l'instance.
ramdiskId	ID du disque RAM associé à cette instance, le cas échéant.
region	Région dans laquelle l'instance est en cours d'exécution.
version	La version du format du Documents d'identité d'instance

Récupérer le Documents d'identité d'instance en texte brut

Pour récupérer le Documents d'identité d'instance en texte brut

Connectez-vous à l'instance et exécutez la commande suivante.

Linux

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-  
metadata-token-ttl-seconds: 21600" ` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/  
instance-identity/document
```

IMDSv1

```
$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/token).Content
```

```
PS C:\> (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

IMDSv1

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

Voici un exemple de sortie.

```
{
  "devpayProductCodes" : null,
  "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
  "availabilityZone" : "us-west-2b",
  "privateIp" : "10.158.112.84",
  "version" : "2017-09-30",
  "instanceId" : "i-1234567890abcdef0",
  "billingProducts" : null,
  "instanceType" : "t2.micro",
  "accountId" : "123456789012",
  "imageId" : "ami-5fb8c835",
  "pendingTime" : "2016-11-19T16:32:11Z",
  "architecture" : "x86_64",
  "kernelId" : null,
  "ramdiskId" : null,
  "region" : "us-west-2"
}
```

Vérifier le Documents d'identité d'instance

Si vous avez l'intention d'utiliser le contenu du Documents d'identité d'instance à des fins importantes, vous devez vérifier son contenu et son authenticité avant de l'utiliser.

Le Documents d'identité d'instance en texte brut est accompagné de trois signatures hachées et chiffrées. Vous pouvez utiliser ces signatures pour vérifier l'origine et l'authenticité du Documents d'identité d'instance et les informations qu'il contient. Les signatures suivantes sont fournies :

- Signature codée en base64 — Il s'agit d'un hachage SHA256 codé en base64 du Documents d'identité d'instance qui est chiffré à l'aide d'une paire de clés RSA.
- Signature PKCS7 — Il s'agit d'un hachage SHA1 du Documents d'identité d'instance qui est chiffré à l'aide d'une paire de clés DSA.
- Signature RSA-2048 — Il s'agit d'un hachage SHA256 du Documents d'identité d'instance qui est chiffré à l'aide d'une paire de clés RSA-2048.

Chaque signature est disponible à un point de terminaison différent dans les métadonnées de l'instance. Vous pouvez utiliser l'une de ces signatures en fonction de vos exigences de hachage et de chiffrement. Pour vérifier les signatures, vous devez utiliser le certificat AWS public correspondant.

Les rubriques suivantes fournissent des étapes détaillées pour valider le Documents d'identité d'instance avec chaque signature.

- [Utiliser la signature PKCS7 pour vérifier le Documents d'identité d'instance](#)
- [Utiliser la signature codée en base64 pour vérifier le Documents d'identité d'instance](#)
- [Utiliser la signature RSA-2048 pour vérifier le Documents d'identité d'instance](#)

Utiliser la signature PKCS7 pour vérifier le Documents d'identité d'instance

Cette rubrique explique comment vérifier le document d'identité de l'instance à l'aide de la signature PKCS7 et du certificat public AWS DSA.

Instances Linux

Pour vérifier le document d'identité de l'instance à l'aide de la signature PKCS7 et du certificat public AWS DSA

1. Connectez-vous à l'instance.

- Récupérez la signature PKCS7 à partir des métadonnées de l'instance et ajoutez-la, ainsi que l'en-tête et le pied de page requis, à un fichier nommé `pkcs7`. Utilisez l'une des commandes suivantes en fonction de la version IMDS utilisée par l'instance.

IMDSv2

```
$ echo "-----BEGIN PKCS7-----" >> pkcs7 \  
&& TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-  
metadata-token-ttl-seconds: 21600" ` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/  
dynamic/instance-identity/pkcs7 >> pkcs7 \  
&& echo "" >> pkcs7 \  
&& echo "-----END PKCS7-----" >> pkcs7
```

IMDSv1

```
$ echo "-----BEGIN PKCS7-----" >> pkcs7 \  
&& curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7  
>> pkcs7 \  
&& echo "" >> pkcs7 \  
&& echo "-----END PKCS7-----" >> pkcs7
```

- Trouvez le certificat public DSA pour votre région dans [AWS certificats publics](#) et ajoutez le contenu à un nouveau fichier nommé `certificate`.
- Utilisez la commande OpenSSL `smime` pour vérifier la signature. Incluez l'option `-verify` indiquant que la signature doit être vérifiée et l'option `-noverify` indiquant que le certificat n'a pas besoin d'être vérifié.

```
$ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee  
document
```

Si la signature est valide, le message `Verification successful` s'affiche.

La commande écrit également le contenu du document d'identité d'instance dans un nouveau fichier nommé `document`. Vous pouvez comparer le contenu du document d'identité d'instance provenant des métadonnées d'instance avec le contenu de ce fichier à l'aide des commandes suivantes.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/document | openssl dgst -sha256
```

Si la signature ne peut pas être vérifiée, contactez AWS Support.

instances Windows

Prérequis

Cette procédure nécessite la classe `System.Security Microsoft .NET Core`. Pour ajouter la classe à votre PowerShell session, exécutez la commande suivante.

```
PS C:\> Add-Type -AssemblyName System.Security
```

Note

La commande ajoute la classe à la PowerShell session en cours uniquement. Si vous démarrez une nouvelle séance, vous devez exécuter à nouveau la commande.

Pour vérifier le document d'identité de l'instance à l'aide de la signature PKCS7 et du certificat public AWS DSA

1. Connectez-vous à l'instance.
2. Récupérez la signature PKCS7 à partir des métadonnées de l'instance, convertissez-la en un tableau d'octets et ajoutez-la à une variable nommée `$Signature`. Utilisez l'une des commandes suivantes en fonction de la version IMDS utilisée par l'instance.

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```


argument(s): "Cannot find the original signer. Si votre signature ne peut pas être vérifiée, contactez AWS Support.

7. Validez le contenu du document d'identité d'instance.

```
PS C:\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Si le contenu du document d'identité d'instance est valide, la commande renvoie True. Si le document d'identité d'instance ne peut pas être validé, contactez AWS Support.

Utiliser la signature codée en base64 pour vérifier le Documents d'identité d'instance

Cette rubrique explique comment vérifier le document d'identité de l'instance à l'aide de la signature codée en base64 et du certificat public AWS RSA.

Instances Linux

Pour valider le document d'identité de l'instance à l'aide de la signature codée en base64 et du certificat public AWS RSA

1. Connectez-vous à l'instance.
2. Récupérez la signature codée en base64 à partir des métadonnées d'instance, convertissez-la en binaire et ajoutez-la à un fichier nommé `signature`. Utilisez l'une des commandes suivantes en fonction de la version IMDS utilisée par l'instance.

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/signature | base64 -d >> signature
```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature | base64 -d >> signature
```

3. Récupérez le Documents d'identité d'instance en texte brut à partir des métadonnées de l'instance et ajoutez-le à un fichier nommé `document`. Utilisez l'une des commandes suivantes en fonction de la version IMDS utilisée par l'instance.

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/  
dynamic/instance-identity/document >> document
```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document  
>> document
```

4. Trouvez le certificat public RSA pour votre région dans [AWS certificats publics](#) et ajoutez le contenu à un nouveau fichier nommé `certificate`.
5. Extrayez la clé publique du certificat public AWS RSA et enregistrez-la dans un fichier nommé `key`.

```
$ openssl x509 -pubkey -noout -in certificate >> key
```

6. Utilisez la commande OpenSSL `dgst` pour vérifier le Documents d'identité d'instance.

```
$ openssl dgst -sha256 -verify key -signature signature document
```

Si la signature est valide, le message `Verification successful` s'affiche.

La commande écrit également le contenu du document d'identité d'instance dans un nouveau fichier nommé `document`. Vous pouvez comparer le contenu du document d'identité d'instance provenant des métadonnées d'instance avec le contenu de ce fichier à l'aide des commandes suivantes.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/  
dynamic/instance-identity/document | openssl dgst -sha256
```

Si la signature ne peut pas être vérifiée, contactez AWS Support.

instances Windows

Pour valider le document d'identité de l'instance à l'aide de la signature codée en base64 et du certificat public AWS RSA

1. Connectez-vous à l'instance.
2. Récupérez la signature codée en base64 à partir des métadonnées d'instance, convertissez-la en un tableau d'octets et ajoutez-la à la variable nommée `$Signature`. Utilisez l'une des commandes suivantes en fonction de la version IMDS utilisée par l'instance.

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
```

3. Récupérez le document d'identité d'instance en texte brut à partir des métadonnées d'instance, convertissez-le en un tableau d'octets et ajoutez-le à une variable nommée `$Document`. Utilisez l'une des commandes suivantes en fonction de la version IMDS utilisée par l'instance.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Trouvez le certificat public RSA pour votre région dans [AWS certificats publics](#) et ajoutez le contenu à un nouveau fichier nommé `certificate.pem`.
5. Vérifier le document d'identité d'instance

```
PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-Path
certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
```

Si la signature est valide, la commande renvoie True. Si la signature ne peut pas être vérifiée, contactez AWS Support.

Utiliser la signature RSA-2048 pour vérifier le Documents d'identité d'instance

Cette rubrique explique comment vérifier le document d'identité de l'instance à l'aide de la signature RSA-2048 et du certificat public AWS RSA-2048.

Instances Linux

Pour vérifier le document d'identité de l'instance à l'aide de la signature RSA-2048 et du AWS certificat public RSA-2048

1. Connectez-vous à l'instance.
2. Récupérez la signature RSA-2048 à partir des métadonnées de l'instance et ajoutez-la, ainsi que l'en-tête et le pied de page requis, à un fichier nommé `rsa2048`. Utilisez l'une des commandes suivantes en fonction de la version IMDS utilisée par l'instance.

IMDSv2

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
&& TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/rsa2048 >> rsa2048 \
&& echo "" >> rsa2048 \
```

```
&& echo "-----END PKCS7-----" >> rsa2048
```

IMDSv1

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \  
&& curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048  
>> rsa2048 \  
&& echo "" >> rsa2048 \  
&& echo "-----END PKCS7-----" >> rsa2048
```

3. Trouvez le certificat public RSA-2048 pour votre région dans [AWS certificats publics](#) et ajoutez le contenu à un nouveau fichier nommé `certificate`.
4. Utilisez la commande OpenSSL `smime` pour vérifier la signature. Incluez l'option `-verify` indiquant que la signature doit être vérifiée et l'option `-noverify` indiquant que le certificat n'a pas besoin d'être vérifié.

```
$ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |  
tee document
```

Si la signature est valide, le message `Verification successful` s'affiche. Si la signature ne peut pas être vérifiée, contactez AWS Support.

instances Windows

Prérequis

Cette procédure nécessite la classe `System.Security` Microsoft .NET Core. Pour ajouter la classe à votre PowerShell session, exécutez la commande suivante.

```
PS C:\> Add-Type -AssemblyName System.Security
```

Note

La commande ajoute la classe à la PowerShell session en cours uniquement. Si vous démarrez une nouvelle séance, vous devez exécuter à nouveau la commande.

Pour vérifier le document d'identité de l'instance à l'aide de la signature RSA-2048 et du AWS certificat public RSA-2048

1. Connectez-vous à l'instance.
2. Récupérez la signature RSA-2048 à partir des métadonnées d'instance, convertissez-la en un tableau d'octets et ajoutez-la à une variable nommée `$Signature`. Utilisez l'une des commandes suivantes en fonction de la version IMDS utilisée par l'instance.

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
```

3. Récupérez le document d'identité d'instance en texte brut à partir des métadonnées d'instance, convertissez-le en un tableau d'octets et ajoutez-le à une variable nommée `$Document`. Utilisez l'une des commandes suivantes en fonction de la version IMDS utilisée par l'instance.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Trouvez le certificat public RSA-2048 pour votre région dans [AWS certificats publics](#) et ajoutez le contenu à un nouveau fichier nommé `certificate.pem`.

5. Extrayez le certificat du fichier de certificat et stockez-le dans une variable nommée `$Store`.

```
PS C:\> $Store =  
[Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog  
Path certificate.pem))
```

6. Vérifiez la signature.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

Si la signature est valide, la commande ne renvoie aucune sortie. Si la signature ne peut pas être vérifiée, la commande renvoie `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer.` Si votre signature ne peut pas être vérifiée, contactez AWS Support.

7. Validez le contenu du document d'identité d'instance.

```
PS C:  
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Si le contenu du document d'identité d'instance est valide, la commande renvoie `True`. Si le document d'identité d'instance ne peut pas être validé, contactez AWS Support.

AWS certificats publics

Les certificats AWS publics suivants peuvent être utilisés pour vérifier le contenu du document d'identité d'une instance, comme décrit dans les rubriques suivantes :

- [Vérifier à l'aide de la signature PKCS7](#)
- [Vérifier à l'aide de la signature codée en base64](#)
- [Vérifier à l'aide de la signature RSA-2048](#)

Assurez-vous d'utiliser le bon certificat pour votre région et pour la procédure de vérification que vous utilisez. Si vous vérifiez la signature PKCS7, utilisez le certificat DSA. Si vous vérifiez la signature codée en base64, utilisez le certificat RSA. Si vous vérifiez la signature RSA-2048, utilisez le certificat RSA-2048.

Développez chaque région ci-dessous pour afficher les certificats spécifiques à chaque région.

USA Est (Ohio) – us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkJ00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQKKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQKKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggEsBgcqhkJ00AQDMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz11r7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MbcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCySfYDk4mZr0LBA4GEAAKBgEbmveve5f8LIE/Gf
MNmP9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAKGBYqGSM44BAMDlwAwLAIUWXB1k40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUUVJTc+h0U+8Gk3J1qsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0
BgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBZXWVzIGU2Vydm1jZXMgTEEx
MB4XDTE0MDQy0TE3MTE0V0V0XDTI5MDQy0DE3MTE0V0VowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAcTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBZXWVzIGU2Vydm1jZXMgTEExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCjVrjF/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfgQ09kZ1wpWpmy08bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBxKtvCcWduUizvtUF2
-----END CERTIFICATE-----
```



```
FwYDVQIQIExBXYXNoaw5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxZzAJBgNVBAYTA1VTMRkwFwYDVQIQIExBXYXNoaw5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggESBgqhkhj00AQBMIIbHwKBgQCjkvcS2bb1VQ4yt/5e
ih5006kk/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MbcJ1/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buyCU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
1Ra2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKml1qx411HW
MXrs3IgiB6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAKGBYqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUE1y2NIKC+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhZGUxEDA0
BgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBxZWVzU2VydmljZXMgTEEx
MB4XDTE0MDQyOTEzMDzQwMVowXDTI0MDQyODEzMDzQwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhZGUxEDA0BgNVBAcTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBxZWVzU2VydmljZXMgTEExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCChvRjF/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJO+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HENf0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXXtvCcwWdUuizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcwWdUuizvtUF2UthYKReMFwxZzAJ
BgNVBAYTA1VTMRkwFwYDVQIQIExBXYXNoaw5ndG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IUE1y2NIKC
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSwb5jT8pYjQb8ZoZkXXRgB09mvYeU
Neq0Br27rvRAnaQ/9LUQf72+SahDFuS4CMI8nowoytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCf0JTpu0temHcFA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBwUAMFwxZzAJBgNV
```

```

BAYTA1VTMRkwFwYDVQIQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEEMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMakGA1UEBhMCMVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBACtB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBxZWVzU2VydmljZXMgTEExMDE1IjBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAs2vqZu9mE0h0q+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
Sfnz+JHQd8WPI+pmNs+q0Z2aTe23k1mf2U52KH9/j1k8R1Ibap/yFibFTSedmegX
E5r447GbJRSHUmuIIfZTZ/orlpuII05/Vz7S0j22tdkdY2ADp7caZkNhxSP915fk
2jJMTBU0zyXUS2rBU/u1NHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQ0JR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjY0Y66LuFzSCXwqSnFBfv
fFBAFsJcGY24G2DoMyYkF3MyZ1u+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHGDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+Pi04qyJ8TWSkwyY4GA1UdIwSBhjCBg4AUryns
Pp4uqSECwy+Pi04qyJ8TWSmhYKReMFwCzAJBgNVBAYTA1VTMRkwFwYDVQIQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6
b24gV2ViIFN1cnZpY2VzIEEMQ4IjALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8LXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcmNrx+g87gAm111z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRiKLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAp1pNRsWAnbP8JB1AP93oJzblX2LQXgykTghMkQ07NaY5hg/H5o4dMPc1TK
LYGq1FUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZwtxwZ0os1jV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitB0w09qBGosCBstwyEqY=
-----END CERTIFICATE-----

```

USA Ouest (Californie du Nord) – us-west-1

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAqQCCQCWukjZ5V4aZzAJBgqhkiG9w0BAQDMFwCzAJBgNVBAYTA1VTMRkw
FwYDVQIQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEEMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJAMFwCzAJBgNVBAYTA1VTMRkwFwYDVQIQIExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEEMQzCCAbcwggEsBgqhkiG9w0BAQBMIIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz11r7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwhHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MbcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buyCU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEEAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgiB6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw

```



```

YXNoaw5ndG9uIFN0YXR1MRAwDgYDVQOHEwdTZWF0dGx1MSAwHgYDVQOKExdBbWF6
b24gV2ViIFN1cnZpY2VzIEExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcv8ZE1XDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9Rj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeH0AZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyX1DiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
lPfhafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawn0TEqcn8m7us=
-----END CERTIFICATE-----

```

USA Ouest (Oregon) – us-west-2

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjz5V4aZzAJBgqhkJ00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXyXNoaw5ndG9uIFN0YXR1MRAwDgYDVQOHEwdTZWF0dGx1MSAwHgYD
VQOKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBXyXNoaw5ndG9u
IFN0YXR1MRAwDgYDVQOHEwdTZWF0dGx1MSAwHgYDVQOKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggEsBgqhkJ00AQBMIIbHwKBgQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0Ca0/buyCU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3carVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKml1qx41lHW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAKGBYqGSM44BAMDLwAwLAIUWXB1k40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFx8PxCKbHwpD31b0yCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWlGU2Vydm1jZXMgTEEx
MB4XDTE0MDQyO0TE3MjM1OVowXDE0MDQyO0TE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWlGU2Vydm1jZXMgTEExDMIGfMA0GCSqGSIb3DQEBAQUA

```

```
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJO+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXXtvCcWdwUuizvtUF2
UTgwGZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcWdwUuizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDVoQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVoQHEwdT
ZWF0dGx1MSAwHgYDVoQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IUfX8PxCKb
HwpD31b0yCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzO1+9Xy1+UsbUBI95H09mbbnduX+aMJXgG9uFZNjgNEBmCvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM405+r7vUa10
dWU+hP/T7DUrPAIVM0E7mpYa+WPWJrN6B1RwQkKQ7twm9kDa1A==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL31rQCSTMMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVoQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVoQHEwdTZWF0
dGx1MSAwHgYDVoQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDEExNzA5MDEzMlowXDELMAKGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhZGUxEDA0BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlU2Vydm1jZXMgTEExDMIIIBjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ260KF+LRPwZfixBH+EbEN/Fx0gYy1jppjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
qWu1q5kmIvYjKGIadfb0U8wLwLcHo8yvvfgI6FiGGsE09VMC56E/hL6Cohko11LW
dizyvRcvG/IidazVkJQCN/4zC9PU0VyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIzSsnRjz3b0cEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fch9FPiFKQNBpiqfAW5Ebp3La13/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVoQIEExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVoQHEwdTZWF0dGx1MSAwHgYDVoQKExdBbWF6
b24gV2ViIFN1cnZpY2VzIEExMQ4IJALZL31rQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCALwEC1pW/f0oRG8nHr1PZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
aBm03SEt5v8mcc7sXWvgFjCnUpz0smky6JheCD401Cf8k0o1Z93FQnTrbg620K0h
83mGCDeVKU3hLH97FY0uq+3N/IliWFDhviBAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRkk=
-----END CERTIFICATE-----
```

Afrique (Le Cap) – af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqWCCQCncbCtQbjuyzAJBgqhkJ00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbYwggErBgcqhkJ00AQBMIIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHMmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2u0tSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
q06TlnExHFVj8LMky1ZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvV05TZKu1IKq7J
gXZr0x/KIT8zsNweetL0aGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAoGAIxOKbVgwLxbn6Pi2
6hB0ihFv16jKxAQI0hHzXJLV0Vv9QwnqjJJRf0Cy3dB0zicLXiIxeIdYfvqJr+u
h1N8rGxEZYjYjEUKMGvsc0DW85jonXz0bNfcP0aaKH01KKVjL+0Zi5n2kn9wgd05
F3CVnM18BUra8A1Tr2yrE6TVZ4wCQYHKOZiZjgEAWmVADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjH1CA=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xOTEwMjQ4
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBACjTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBxZWVzU2VydmljZXMgTEExDMIGFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfW1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlyqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxSybC3ziPYaHI42UiTkQNAhmoRoNeqVyHNnBpQIDAQAABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLy1Wye1Eg0pW4B1XPyRVD4pAds8Guw2+krqgkY0HxLCdjosuH
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbP0nokhKTMpXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```

MIID0zCCAi0gAwIBAgIJAIIFI+05A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWw6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAGT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBACjTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBxZWV2VydmljZXMgTEExMIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIB
CgKCAQEAY7/WHBBH0rk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnfhij2w0cQdbLandh0EGtbxerete3IoXzd1KXJb11Pvmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYU3KLxfqAdTVhuC0NRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTVw2
9Qr7QBjjB0VbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oC0QNoG1v5XbHJe2o
JFD8GRRy2rkW0/1NwVFDcweC6zC3QwIDAQAABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSB0fBjsfFu1yg1Zgn2nDCK7kQhx
jMjMNIvXbbs3yMqQ2cHUKkCkF5t+WldfeT4VklRz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmmx5XS7W0SCN0oAxW
EH9twibauv82DVg1W0kQu8EwFw8hFde9X0Rkiu0qVcuU81JgFEvPWMDFU5sGB6ZM
gkEKTzMvLZpPbBhg99Jl
-----END CERTIFICATE-----

```

Asie-Pacifique (Hong Kong) – ap-east-1

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQC07MJe5Y3VLjAJBgqhkiG9w0BAQMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWw6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWw6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbgwggEsBgqhkiG9w0BAQMIIBHwKBgQDvQ9RzVvf4MAwGbbqfX
b1CvCoVb99570kLGN/04CowHXJ+vTBR7eyIa6AoX1tsQXB0mrJswToFKKxT4gbuw
jK7s9QX4CmTRwEg02RxtZSVj0hsUQmH+yf7Ht40VL97LWnNfGsX2cwjCRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGkd9FAoGBA0CG
eSNmXpW4QFu4pI1Aykm6EnTZKKHT87gdXkAkfoC5fAf0xxhnE2HezZH9Ap2tMV5
8bWnvoPHvoKCQqwfM+OUB1AxC/3vqoVklL2mG1KgUH9+hrtpMTkw03RREnKe7I50
x9qDimJp0ihrl4I0dyvy9xU0oz+DzFAW8+y1WVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz61AZLedeBKpaP53Z1DT034J0C55YbJTwBTFGqPt0LxnUVD1GiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pd0u/ibRPH11E2nz6pK7G60QtLyHTAJBgqhkiG9w0BAQDAzAAMC0CFQCoJlWgtJQC
cLoM4p/jtVF0j26xbgIUUS4pDKyHaG/eaygLtTfPjJqzWHC=
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBjb250bW9uMR0wGAYDVQQDExF1YzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTA1VTMRMw
EQYDVQQIEWpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGx1MRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXyTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXf1UpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPhuGILDyaNN
dKcvp1NFwDTydvG32MNubAGnecoEBtUPtxBsLoVYXC0b+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaB0ntQbX9bgHiUxw6XZWaTS/6xjRJD5p3S1E0mPI31P/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----

```

RSA-2048

```

-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEwBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24uY29tIEluYy4xIFN1cnZpY2VzIEExMQZAgFw0x
ODA3MjAwODQ0NDRAgA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24uY3RhdGUxEDA0BgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBxZWVjZjYydm1jZXMgTEExIjANBgkqhkiG9w0BAQEFAAOCQAQ8AMIIB
CgKCAQEA4T1PNs0g0FDrG1WePoHe0Sm0JTA3HCry5LSbYD33GFU2eBr0IxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbx
Fz4uwBIN3/drM0RSbe/wP9EcgMNUGQMMZWeAji8sMtwp0b1NWAP9BniUG0F1cz6Dp
uPovwDTLdAYT3TyhzlohKL3f6048TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHn74Kdq35UgrUxNhJraMGczzno1UuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgty0FX/I3Cyk+Pui44Ig0wCsIdNGwuJysdq5VIfnjegEu2zIMWJSKG0
lMzoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WE0fn0/CbMuf/x99CckNDwpjgW+
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TI1c/qUceBycrIQ/kke
jDFsihUMLqgm0V2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLft5SbsGdUA3AUy1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0zJ1
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----

```


RSA-2048

```

-----BEGIN CERTIFICATE-----
MIIIEejCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXyXNoaw5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0yMjA0MDgX
MjM5MTZaGA8yMjAxMDkxMjE5MzcxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBACTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlU2Vydm1jZXMgTEExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
Tv0yYNNiZKTHWmzmulmdinWNbwP0GiR0Hb/i7ro0HhvnptyycGt8ag8affiIbx5X
7ohdwSN2KJ6G0IKf1Ix7f2NEI0oAMM/9k+T1eVF+MVWzpzoiDp8frLNkqp8+RAgz
ScZsbrfWv3u/if5xJAVdg2nckIWDMSHEVPoz01Jo7v0ZuDtWwSL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36o0dDwvZpqY1kLi3uxZ4ta+a
01pz0STwMLgQZSbKWQrPmvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExB
YXNoaw5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6
b24gV2ViIFN1cnZpY2VzIEExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxLZT0ba
6wTMzk7c3akb6XM0SZFbGaiFkebPZqTHEhD1rC1M2j9AI1YcCx6YCrTf4cuhn2mD
gcJN33143e0WSaeRY3ee4j+V9ne98y3k02wLz95VrRgc1PFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2q0cDuRGaikdS+dYaLsi5z9cA3FolHzWxx9M0s8io8vKqQzV
XUrlTNWwuhZy88c0lqGPxnoRbw7TmifwPw/cunNrsjUU0gs6ZTk=
-----END CERTIFICATE-----

```

Asie-Pacifique (Melbourne) ap-southeast-4

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDA0
U4EddRipUt9KnC7s50f2EbdSP09EAMMeP4C2USZpRV1AI1H7WT2NWPq/
xfw6MPbLm1Vs14E7gB00b/JmYLdirmVC1pJ+f6AR7ECLCT7up1/63xhv401fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUA12BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v60uqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBGLRjFnEj6EwoFh03zwykjMim4TwWeotUfI0o4K0uHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZ16Ae1U1LZAFM0/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXK1rgBgEVCprLHdK/bbrMas0XMu1Eh0D

```


Asie-Pacifique (Mumbai) – ap-south-1

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAqQCCQCWukjZ5V4aZzAJBgqhkJ00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEiExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQKKExdBbWF6b24gV2ViIFN1cnZpY2VzIEEMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEiExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEEMQzCCAbcwggEsBgcqhkJ00AQBMIIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MbcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDlwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAOqgAwIBAgIUdLA+x6tTAP3LRT1r0z6n0xfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0
BgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBxZWVzIGU2Vydm1jZXMgTEEx
MB4XDTE0MDQyOTE0MTMwMVowXDTI1MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAcTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBxZWVzIGU2Vydm1jZXMgTEExDMIGFMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HENf0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHGDAdBgNVHQ4EFgQUJdbMCBXXtvCcWdwUuizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcWdwUuizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDVQQIEiExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEEMQ4IUDLA+x6tT
AP3LRT1r0z6n0xfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQAZ7rYKoAwwiiH1M5GJbrT/BEk3002VrEPw8ZxgppQ/EK1zML0s/0Cyimp7
UYyUgYfQe5nq37Z94r0USeMgv/WRxaMwrL1LqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIH0pQocJUS1m/dLeMuE0+0A3HNR6JVktGsUdv9u1mKw==
-----END CERTIFICATE-----

```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIID0zCCAi0gAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXlYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAGT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBhZG90b24gU3RhdGUxIDAeBgNVBAoTF0FtYXpvbiBhZG90b24gU3RhdGUx
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79m0x0AbeWg91Ka0D0zw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIw1Bpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGh1LxLHLms0IxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNL2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBIE
6w+WWC2gCfoJ06c9HMyGLMFEpqZmz1n5IcQt1h9iy07Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3S0Ea070IMCFwkus05f61e0yFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysV1qyT9WZd7E0Ym5j5oue2G2xdei+6etgn5UjyWm6liZGrc0F6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ10VLztIfSN5J40o1pu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2Cc1Choz8XDQcvvKAh
```

```
-----END CERTIFICATE-----
```

Asie-Pacifique (Osaka) – ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkJ00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXlYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAzMDcxMDQ1MDFaGA8y
MTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAGTJ0FtYXpvbiBhZG
90b24gU3RhdGUxEDA0BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBhZG90
b24gU3RhdGUxIDAeBgNVBAoTF0FtYXpvbiBhZG90b24gU3RhdGUxIDAeBgNVBAoTF0
FtYXpvbiBhZG90b24gU3RhdGUxIDAeBgNVBAoTF0FtYXpvbiBhZG90b24gU3RhdGUx
cnZpY2VzIEExMQzCCAbcwggEsBgqhkJ00AQBMIIIBHwKBGCjKvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmve5f8LIE/Gf
```

```
MNmP9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgiB6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDlwAwLAIUwXB1k40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZF0GvTFKxHoy9+f5H18wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0
BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBxZWVlZjZXMgTEExDQYJKoZI
MB4XDTE0MDQyOTE2NTQwN1oXDTE1MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBxZWVlZjZXMgTEExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHGdAdBgNVHQ4EFgQUJdbMCBXXtvCcWdwUuizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcWdwUuizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDVoQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVoQHEwdT
ZWFOdGx1MSAwHgYDVoQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IUHTRhxHhB
ZF0GvTFKxHoy9+f5H18wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUz7DcYbhWNTD4BNGhr5beruT20UoGHH9J73UKxwdqeb9bH1LIWhIZ00X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBry8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXEN1kC04v5yxdKxZxyg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVoQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVoQHEwdTZWFO
dGx1MSAwHgYDVoQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI10FowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBxZWVlZjZXMgTEExDMIEIIBiANBgkqhkiG9w0BAQEFAA0CAQ8AMIIB
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YwTHNwaM91z
zmyK6Sk/tK1Wxcn13g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnyVwd4D6erLl/ENijeR10xVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyZAjUmklcqTfMfPckzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzg007Z2SAE63PI048JK8Hc0bh
tXORUQ/XF1jzi/SIaUJZT7kq3kwl8wIDAQABMA0GCSqGSIb3DQEBwUAA4IBAQBj
```

```

Tht09dLvU2QmKuXAhxXjsIdl1QgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8Q0MGYfGdYkcoBjsgiyvMJU/2N2UbZJNGWvcEGkdjGJUYY00
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9G1q/9n
izPrI09hMypJDP04ugQc
-----END CERTIFICATE-----

```

Asie-Pacifique (Séoul) – ap-northeast-2

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkJ00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEyBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQKKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEyBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQKKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggESBgqhkJ00AQBMIIIBHwKBQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkmVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJ1/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buyCU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
1Ra2v1ntMX3carVdDbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKml1qx41lHW
MXrs3IgiB6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAKGBYqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbsSn2UI06vYk4iNwV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBxZWVzIGU2Vydm1jZXMgTEEx
MB4XDTE0MDQy0TEzZmZg0N1oXDTI5MDQy0DEzZmZg0N1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBxZWVzIGU2Vydm1jZXMgTEExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvrjF/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwUB/dcnIob6w420k9WY5C0IIGtDRNauN3ku

```

```
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAWIHgDAdBgNVHQ4EFgQUJdbMCBXXtvCcWdUUIzvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcWdUUIzvtUF2UTihYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IUBBSn2UIO
6vYk4iNwV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQAmjTja1G8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlFRtc20wPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUh02+xVRXDxVxM/V0bFgPERbJpyA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJANuCGcCht0JhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWFO
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBxZWlgaU2Vydm1jZXMgTEExMjI1MjI1MjI1MjI1MjI1MjI1MjI1MjI1MjI1
CgKCAQEA66iNv6pJPmGM20W8HbVYJS1KcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMD1rJckDDk6dxU0hmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
m06QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vi14
9FjWS8XmMNwFT1Shp411TDTeVdWw/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/F1ghnSnK105ZKj+b+KI3adBL80MCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
mA4q+12pxy7By6g3nBk1s34PmWikNRJBw0qhF8ucGRv8aiNhRRye9lokXomwo8r
KHbbqvtK8510xUZp/Cx4sm4aTgcMvfJJP29jGLc1DzeqADIVkWEJ4+xncxSYV1S9x
+78TvF/+8h9U2LnS164PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfn
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy81ki0svU9XzUaZ0fZSfXX
wXxZamQb0NvFcxVHY/0PSiM8nQoUmkkBQuK1eDwRWvkoJKYKyr3jvXK7HIWtMr04
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----
```

Asie-Pacifique (Singapour) – ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqQCCQCWukjZ5V4aZzAJBgqhkiG9w0BAQDAQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWFOdGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjI1MjI1MjI1MjI1MjI1MjI1
-----END CERTIFICATE-----
```

```

ODAxMDUxMjU2MTJaMFwxZzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIEExMQzCCAbcwggEsBgqhkhj00AQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MbcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buyCU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
1Ra2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKml1qx41lHW
MXrs3IgiB6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAKGBYqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXng1Wf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0
BgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBZXWV2VydmljZXMGTEExD
MB4XDTE0MDQyOTE0MzAxNFoXDTI1MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAcTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBZXWV2VydmljZXMGTEExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvrjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnf0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXXtvCcwduUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcwduUizvtUF2UTihYKReMFwxZzAJ
BgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEExMQ4IUSqP6ih++
+5KF07NXng1Wf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBGQAw13Bxw11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750M0cP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNck+5GZG4Xec5DoapBZHxmfm093sjxBFP
4x9rWn0GuwAV09ukjYpEvq2Rerilrq5VvppHtbATVNY2qecXDA==
-----END CERTIFICATE-----

```

RSA-2048

```

-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAjVMGw5SHkcvMA0GCSqGSIb3DQEBcwUAMFwxZzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEExMQzAgFw0xNTEwMjkw

```

```

ODU3MT1aGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCMVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWVlU2VydmVjZXMgTEExDMIIIBjANBgkqhkiG9w0BAQEFAAOCQAQ8AMIIB
CgKCAQEAlaSSLfBl70gmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjKuyOyfET50AyT43jTzDPHZTkRSVkyjBdcYbe9o/0Q4P7IVS3
X1lvwrUu0qo9nSID0mxMn0oF1l8KAqnn10tQ0W+1NSTkasW7QVzcb+3okPEVhPA0q
Mn1Y3vkMQGI8zX4i0KbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
R0g415kLYcodjqThmGJPNUpAZ7M0c5Z4pymFuCHgNAZNvjhZDA8420jecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtY0Ij7b0QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQOIEExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6
b24gV2ViIFN1cnZpY2VzIEExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZK5rca8o0P0VS+to1JJE/FRZO
atH0eaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIVYM4LZYImLGuvo0
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQ1RTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5Wu0r8unKj7YxdL1bv7//RtVYVVVi2961doRUYv45CvJF11z00dQ=
-----END CERTIFICATE-----

```

Asie-Pacifique (Sydney) – ap-southeast-2

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkiG9w0BAQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQOIEExBXyXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAxMDUxMjU2MTJhFw0z
ODAxMDUxMjU2MTJhMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQOIEExBXyXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggEsBgqhkiG9w0BAQMIIBHwKBQCjKvcS2bb1VQ4yt/5e
ih5006kK/n1Lz11r7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MbcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buyU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmveve5f8LIE/Gf
MNmP9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3Igb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIzizqQYMAkGByqGSM44BAMDLwAwLAIUWXB1k40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K

```



```
AQAwdQYJKoZiHvcNAQELBQADggEBACobLvJ8Ix1Qy0RTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYpEFTgdWB9W3YCNc34Ss9TJq2D7t/zLGG1bI4wYXU6VJjL0S
hCjWeIyBXUZ0ZKFCb0DSJeUElsTRSXSfUvZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiiJFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfbk6trP8fUVYLHLsV1Iy51Gx+tgwFEYkG1N8I00/
2LCawwaWm8FYAFd3IZ104RImNs/IMG7VmH1bf4swH0BHgCN1uYo=
-----END CERTIFICATE-----
```

Asie-Pacifique (Tokyo) – ap-northeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkJ00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEyBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQKKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEyBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQKKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggEsBgqhkJ00AQBMIIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJ1/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buyCU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
1Ra2v1ntMX3carVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQ0Gx5ho8Wqd+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKml1qx41lHW
MXrs3IgiB6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAKGBYqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZiHvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBxZWVudjU2VydmljZXMgTEEx
MB4XDTE0MDQyOTYyMjU2MTU2MDQyOTYyMjU2MTU2MDQyOTYyMjU2MTU2MDQyOTYy
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBxZWVudjU2VydmljZXMgTEExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvrjF/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
-----END CERTIFICATE-----
```

```
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAWIHgDAdBgNVHQ4EFgQUJdbMCBXXtvCcWdUUIzvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcWdUUIzvtUF2UTihYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IULgwDh7Ti
DrPPBJwscqDwiBhKEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQBtjAg1Bde1t4F9EHCZ0j4qnY6Gigy070u54i+1R77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro10VY11HmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0Bj0C
gepj11UoiN70A6PtA+ycN1sP0oJvdBjhvayLiuM3tUfLTrgHbw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIIEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZW
FdGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IULgwDh7Ti
DrPPBJwscqDwiBhKEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQBtjAg1Bde1t4F9EHCZ0j4qnY6Gigy070u54i+1R77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro10VY11HmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0Bj0C
gepj11UoiN70A6PtA+ycN1sP0oJvdBjhvayLiuM3tUfLTrgHbw==
-----END CERTIFICATE-----
```

Canada (Centre) – ca-central-1

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkJ00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQKKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQKKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggEsBgcqhkJ00AQBMIIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKml1qx41lHW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDlwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAOqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMVCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0
BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBxZWVzIGU2Vydm1jZXMgTEEx
MB4XDTE0MDQyOTE1MzU0M1oXDTE1MDQyODE1MzU0M1owXDELMAkGA1UEBhMVCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBxZWVzIGU2Vydm1jZXMgTEExDMIGFMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXXtvCcWdwUuizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcWdwUuizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQKKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IUIrLgixJJ
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQBHIQJmzyFAaSYs8SpiRijIDZW2RIo7qBkb/pI3rqK6y0WD1PuMr6yNI81D
IrkGgftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwdhdhKYy4BhteFQl/Wex3xTLX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iy0Wrrz/jVxwq7T0kCw==
-----END CERTIFICATE-----

```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIID0zCCAi0gAwIBAgIJAJNKHJhaJ0uMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWV6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBACTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBZXWV2VydmljZXMgTEExDMIIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIB
CgKCAQEAAhDuh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY819XoHndnxmP50Cqld
+26AJt1t1qHpI1YdtnZ60rVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWhA9ln
InHbToLX/SWqBHL0X78HkPRaG2k0C0HpRy+fG9gvz8HCiQaXCbWNFDHZev90ToNI
xhXBVzIa3AgUnGma1CYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUCM00
LBvmTGGeWhi04MUZwf0kwn9JjQZuyLg6B10D4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUb17Bh9pvzFR5gJN1pjm2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAj
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEozwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTam0sguuPrhVp1120gRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h60p5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd70zuSEJ+mBxmzxSjSwM840oh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
```

```
-----END CERTIFICATE-----
```

Canada Ouest (Calgary) – ca-ouest-1

DSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAKGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
U4EddRIpUt9KnC7s50f2EbdSP09EAMMeP4C2USZpRV1AI1H7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLd1mVClpJ+f6AR7ECLCT7up1/63xhv401fnxqimFQ8E
+4P208UewwI1VBNAfPey9nXzrith1yrv8iIDGZ3RSAHHAhUA12BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmU17v60uqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFh03zwyjMim4TwWeotUfI0o4K0uHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZL6Ae1U1ZAFM0/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRS1FQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZiZjgEAWMvADAsAhRjC4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvP1mGPupP1GiHe0veZi08=
```


Europe (Francfort) – eu-central-1

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAqQCCQCWukjZ5V4aZzAJBgqhkj00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEiExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQKKExdBbWF6b24gV2ViIFN1cnZpY2VzIEEMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwCzAJBgNVBAYTA1VTMRkwFwYDVQQIEiExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEEMQzCCAbcwggEsBgcqhkj00AQBMIIIBHwKBQCjKvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MbcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDlwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAOqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMVCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0
BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBxZWVzIGU2Vydm1jZXMgTEEx
MB4XDTE0MDQyOTE1NTUyOVVoXDTI1MDQyODE1NTUyOVowXDELMAkGA1UEBhMVCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBxZWVzIGU2Vydm1jZXMgTEExDMIGFMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HENf0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXXtvCcWdwUuzvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcWdwUuzvtUF2UTihYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDVQQIEiExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEEMQ4IUF5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQBbH0WaX1BsW56Hqk588MmJxs0rvcKfDjF57RgEDgnGnQaJcStCVWD09UY0
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
0/LY0VHCknuPL123VmVRNs51qQA9hkPjvw21UzpdLxaUxt9Z/w==
-----END CERTIFICATE-----

```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXlYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDEExNzA5MDgxOVowXDELMAKGA1UEBhMCMVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhZGUxEDA0BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWV2VydmljZXMgTExDMIIIBIjANBgkqhkiG9w0BAQEFAAOCQAQ8AMIIB
CgKCAQEAKa8FLhxs1cSJK+Q+q/vTf8zVnDAPZ3U6oqpp0W/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqN15H/4U/Q/fr+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4V03TuKy+rZXYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909s14ZAUh+qIYfZK85DAjm
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izzZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRf1gu3MudN6zTuP6YehYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBX
lYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4I
JAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5Z1MJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AF0/6pQDdPxXn3xBhF0mTKPr0GdvYmjZUtQMSVb91bMWCFFs
w+SwDLnm5NF4yZchIcTs2fdpoyZp0HDXy0xgx01gWhKTnYbaZ0xkJvEvckcxVAwJ
obF8NyJ1a0/pWdjh1HafEXEN81xyTTY0a0BGTuY0BD2cTYynauVKY4fqHUKr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvq1codbpsS0huGNLzh0Q=
```

```
-----END CERTIFICATE-----
```

Europe (Irlande) – eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkj00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXlYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAxMDUxMjU2MTJhFw0z
ODAxMDUxMjU2MTJhMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBXlYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggEsBgqhkj00AQBMIIIBHwKBGQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```

hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MbcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDlwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0
BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBxZWlgaU2Vydm1jZXMgTEEx
MB4XDTE0MDQyOTE2MTg0MDU0ODU0ODU0ODU0ODU0ODU0ODU0ODU0ODU0ODU0ODU0
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBxZWlgaU2Vydm1jZXMgTEExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQChvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHGDAdBgNVHQ4EFgQUJdbMCBXXtvCcWdwUuizvtUF2
UTgwgZkGA1UdIwSBKTCBjoAUJdbMCBXXtvCcWdwUuizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDQ0EIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDQ0QEwdT
ZWf0dGx1MSAwHgYDQ0QEExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQADIKn/MqaLGPuK5+prZZ50x4bBZLPtre02C7r0ppqU2kPM21VPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYYvir5r/yDmWzx+BvH5S/g==
-----END CERTIFICATE-----

```

RSA-2048

```

-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJA0rmqHuaUt0vMA0GCSqGSIb3DQEBwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDQ0EIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDQ0QEwdTZWf0
dGx1MSAwHgYDQ0QEExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOjV0VowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBxZWlgaU2Vydm1jZXMgTEExDMIEIIBjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIB
CgKCAQEAEjE7nVu+aHLtZp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECctc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvf1twu9AR0VT22dU0TvERdkNzveoFCy

```

```

hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP90+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83CsglibeK54HP9w+FsD6F5W+6ZSHGJ881
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI50ltBbcPF4c7Y20j0IwwI2Sg0QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHGDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwCzAJBgNVBAYTA1VTMRkwFwYDVQQIEsBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6
b24gV2ViIFNlcnZpY2VzIEExMQ4IJA0rmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAgm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qn05usUKAeQsa+kZIJPyEri5i8LEodh46DAF1R1XTMYgXXx10YggX88XPmPtok17
14hib/D9/lu4IaFIyLzYNSzsETyWkWoGve7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nR0on79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPziKzqWa87xh2DbAyyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KwkdNudGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----

```

Europe (Londres) – eu-west-2

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkJ00AQDMFwCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEsBXN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6
b24gV2ViIFNlcnZpY2VzIEExMQ4IJA0rmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAgm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qn05usUKAeQsa+kZIJPyEri5i8LEodh46DAF1R1XTMYgXXx10YggX88XPmPtok17
14hib/D9/lu4IaFIyLzYNSzsETyWkWoGve7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nR0on79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPziKzqWa87xh2DbAyyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KwkdNudGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----

```

RSA

```
-----BEGIN CERTIFICATE-----
```


Europe (Milan) – eu-south-1

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCME1HPdwG37jAJBgqhkhj00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEiExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEiExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbYwggErBgcqhkhj00AQBMIIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xN0nU7+2eVQtEqjFbDADFENh1p3sh9Q90oheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ30LaVGd1PMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NL0S4326eFRUT+4ornQFjJjP6dp3p0BEzpImNmZTtkCNNUKE4Go9hv5T41h
R0p0DvWv0CBupMAZVBP90bp1XPCyEIZtuDqVa7ukP0UpQNgQhLLAqkigTyXV0Smt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV10EQPYUg5/M3xf
6vE7jKTxxyFWEyjkfJK7PZCz0IGrE/swgACy4PYQW+AwcUweSlK/Hx20aZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8v0BeLv
uaMQmg0YeZ5e0f104GtqP1+lhcQwCQYHkoZIZjgEAwMwADAtAhQdoeWlRkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0t0m08
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJA0Z3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEiExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xOTEwMjky
NTE5MDlaGA8yMTk5MMDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhhdGUxEDA0BgNVBAClTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBxZWlgaU2Vydm1jZXMgTEExDMIGFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEC4nPIGoUo1pAXcjFhWp1o20+
ivgfCsc4AU90pYdAPha3spLey/bhHPri1JZHRNqSckP0hzcCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/f1JFBJ6JHhp0KwM81XQG591V6kkow7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRX1KdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW10tZkiHwCQcn0ttz+8vpew
wx8JGMvowtuKB1iMsbwyrqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----

```

RSA-2048

```

-----BEGIN CERTIFICATE-----

```

```

MIID0zCCAiOgAwIBAgIJA0/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAGT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBACjB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBZXWV2VydmljZXMgTEExDMIIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB61rRxKhhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpql035tJQD+NJuqFd+nXrtcw4yGtmvA6w1
5Bjn8WdsP3x0TKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qz1RTzLapXp4/5
iNwusrTNexG18BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvartvZwV8G1VZt0CGPtNv0i4AR/UN6Tmm51BzUB5nurB4z0R2MoYO
Uts9sLgVsfALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmeP456XXc058MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCsd+XPifXay690FlsCIgLim11HgPkRIHE0XLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvg1waMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN80Xq
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----

```

Europe (Paris) – eu-west-3

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkiG00AQMDFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjY0MjY0MjY0MjY0MjY0
ODAxMDUxMjY0MjY0MjY0MjY0MjY0MjY0MjY0MjY0MjY0MjY0MjY0MjY0MjY0MjY0
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggEsBgqhkiG00AQBMIIBHwKBgQCjKvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJ1/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buyCU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAKGBYqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```



```
-----END CERTIFICATE-----
```

Europe (Espagne) – eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAGMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9Knc7s50f2EbdSP09EAMMeP4C2USZpRV1AI1H7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdirmVC1pJ+f6AR7ECLCT7up1/63xhv401fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzriith1yrv8iIDGZ3RSAHHAhUA12BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v60uqC+VdMCz0HgmdRWVe0utRZT
+ZxBxCBgLRJFnEj6EwoFh03zwyjMim4TwWeotUfI0o4K0uHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZ16Ae1U1ZAFM0/7PSSoDgYQAaOGAGG2m8EKmaf5qQqj3Z
+rzSaTaXE3B/R/4A2VuGqRYR7M1jPtwdmU6/3CPjCACcZmTic0AKbFiDhQadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8q0U7oZ0UWK41biAQs1MihoUwCQYHKoZiZjg
WmbaU7YM5GwCFCvIJ0es05hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIICmzCCAzygAwIBAgIGAXjwLkiaMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIDDBBYXNoaW5m
VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIbSdbWFhA3fi5ippjKkh3s18VyCvCOUXKd0aNrYBrPRkrdH
+3m/
rxIUZ2IK1fD1C6sWAjddf6sBrV2w2a78H0H8EwuwiSggtURBjwJ7KPPJCqaqrQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
+FzqQDzun/
iMMzcFucmL15BxEb1rFX0z7IIu0eiGkndmrquEDCykztLku45s7hxdNy41tTuVAaE5aNBdw5J8U1mRvsKvHLY2ThH6h
+hBgiphYp84DubWVYeP8YqLEJSqscKscWC
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIIEEjCCAvqgAwIBAgIJALWsm06DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKEXdBbWf6b24gV2ViIFN1cnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAGT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlGdU2Vydm1jZXMgTEExMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```

CgKCAQEAuAAhuSpsHC00/fD2zN1BDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZC0sbpPZ+i74N0EQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNV1xYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9012xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph01baqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
i1o8kr+tbIF+JmcgYLBv08Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHGDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhqYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDQVQIEExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDQVQHEwdTZWF0dGx1MSAwHgYDQVQKExdBbWF6
b24gV2ViIFN1cnZpY2VzIEExMQ4IJALWSm06DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFwEhAmtrwyE/i6FDSIphDrMHBkw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtC10ZL5WJiJwel8eDSg+sqJUxEO1
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHE0VP7Zk9C2ehrBXZCMLSdt3GV
fEuMea2RxMhoz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILp0ZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----

```

Europe (Stockholm) – eu-north-1

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkj00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDQVQIEExBXNoaW5ndG9uIFN0YXR1MRAwDgYDQVQHEwdTZWF0dGx1MSAwHgYD
VQVQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJAMFwxCzAJBgNVBAYTA1VTMRkwFwYDQVQIEExBXNoaW5ndG9u
IFN0YXR1MRAwDgYDQVQHEwdTZWF0dGx1MSAwHgYDQVQKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEExMQzCCAbcwggEsBgqhkj00AQBMIIbHwKBGQCjKvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buyU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDlwAwLAIUWXB1k40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```



```
-----END CERTIFICATE-----
```

Europe (Zurich) – eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAKGBYqGSM44BAMwXDELMakGA1UEBhMCMVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s50f2EbdSP09EAMMeP4C2USZpRV1AI1H7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdirmVClpJ+f6AR7ECLCT7up1/63xhv401fnxqimFQ8E
+4P208UewwI1VBNAfEy9nXzriith1yrv8iIDGZ3RSAHHAhUA12BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v60uqC+VdMCz0HgmdRWVeOutRZT
+ZxBxBcBGLRjFEnEj6EwoFh03zwyjMim4TwWeotUfI0o4K0uHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZ16Ae1U1ZAFM0/7PSSoDgYQAAoGAYNjaCNg/
cfGQ011BUj5C1Uu1qwZ9Q+SfDzPZH9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjvvt2Ch//
b+sZ86E5h0XWwR+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDt1L8X/
Rpfalu2Z20JgjFJWGf7hRwx456n
+lowCQYHkoZIZjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIICmzCCAZygAwIBAgIGAXjSGFGiMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIDDBBXyXNoaW5m
opKZAUusJx2hpgU3pUhh1p9ATh/VeVD582jTd9IY
+8t5MDa6Z3fGliByEiXz0LEHdi8MBacLREu1TwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAIL1poE3k9o7KdALAxSfJNi
+g3RMzdbiFM+7MA63Nv5fsf+0xgcjSNBE1vPCDKFvTJ14QQhToy0561105GvdS9RK
+H8xrP2mrqngApoKTApv93vHBixgFSn5KrczR00YSm30jkqbydU7DF1mkXXR7GYE+5jbHvQHYiT1J5sMu
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBQwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXyXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKEXdBbWf6b24gV2ViIFN1cnZpY2VzIExMQzAgFw0yMjA3MTgx
NTEyMDdaGA8yMjAxMTIwN1owXDELMakGA1UEBhMCMVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlU2Vydm1jZXMgTEExIjANBgkqhkiG9w0BAQEFAAOCQA8AMIIB
CgKCAQEAYn+Lsnq1ykrfY1Zkk6aAAYNRend9Iw8AUwCBkg0r2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpgHioamcYhrPXyIxlWiRQ1aqSg
```

```

OFiE9bsqL3rCF5Vz+t0iTe5W/7ojf0Fls6++g7ZpobwJlpMbuJepqyeHMPyjv05A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9k13IOQrsLshBB5fFUj109NiFipCGBwi+8ZMeSn1
5qwBI01BWXPFg7WX60wyjhmh6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6
b24gV2ViIFNlcnZpY2VzIEExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG1HYDtchPfbvdHx9HEQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtr0d9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMV1SQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978WY9ccXwVSeYG/YAr5rJpS6ZH7ERQvUY0IzwFNea0Pg0TEVpcjW1V6+MQEvsEx
W85q+s6AVr49eppEx8SLJs10C23yB+L+t32tAveQImRwTJmpzZ5cxh/sYgDVeOC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHG0AmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----

```

Israël (Tel Aviv) – il-central-1

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGBYqGSM44BAMwXDELMakGA1UEBhMCMVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBACMB1N1YX
U4EddRIPUt9KnC7s50f2EbdSP09EAMMeP4C2USZpRV1AI1H7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdirmVC1pJ+f6AR7ECLCT7up1/63xhv401fnxqimFQ8E
+4P208UewwI1VBNAFpEy9nXzriith1yrv8iIDGZ3RSAHHAhUA12BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v60uqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFh03zwyjMim4TwWeotUfI0o4K0uHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZ16Ae1ULZAFM0/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgj0oUwWdl6fj1zWca
pq+11ezuK2DF0zNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jKpXsvrS
+xTo2M9h2s2uLAhEQIU0Z2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIICmzCCAZygAwIBAgIGAX0QQGVLMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIDDBBXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFNlcnZpY2VzIEExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG1HYDtchPfbvdHx9HEQE8HgNugJUPdEqxunt9U33p8VFrs+uLPtr0d9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMV1SQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978WY9ccXwVSeYG/YAr5rJpS6ZH7ERQvUY0IzwFNea0Pg0TEVpcjW1V6+MQEvsEx
W85q+s6AVr49eppEx8SLJs10C23yB+L+t32tAveQImRwTJmpzZ5cxh/sYgDVeOC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHG0AmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----

```



```
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkw2HWASyND17bAoGBANTz
Idhfmq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL31Tm0Nne1r19yGujrjQwy5
Zp9V4A/w9w2010Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Y16L1300HQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+G0/LpCA4GFAAKBgQCVS7m77nuNALZ8
wvUqcooxXMPkxJF154NxAsAu19KP9KN4svm003Zrb7t2F0tXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFwSrTgTzPE3p6U5ckcgV1TAJBgcqhkj00AQDAy8AMCwCFB2NZGwm5ED1
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAM16uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIXCzAJBgNV
BAYTA1VTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGx1MSAw
HgYDVQQKDBdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzEaMBGGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTEwNDIyMTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIX
CzAJBgNVBAYTA1VTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGx1MSAwHgYDVQQKDBdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzEaMBGGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0Z1pY5y3Kno0reCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQ1cq81DB1GmXehRkZRgGeRge1ePwD1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NN1+vynyi0wUUr7/wIZTAgMBAAGjgdwgdQwHQYDVR00
BBYEFILtMd+T4YgH1cgc+hVsV0V+480FMIGkBgNVHSMGZwwgZmAFILtMd+T4YgH
1cgc+hVsV0V+480FoXakdDBYMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFd1YiBTZXJ2
aWN1cyBMTEMxGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0BAQsFAA0BgQBhKNTBIFgWfd+ZhC/LhRUY
40jEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKD08rNE84jqxrxRsfdi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJANZkF1QR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXyXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzEaMBGGA1UEAwwR
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAKGA1UEBhMVCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWVudm1jZXMgTEExMjE1IjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIB
CgKCAQEAY4Vnit2eBpEjKgOKBmyupJzJAI4fr74tuGJNwwa+Is2vH12jMzn9I11
```

```
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiI1kUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDF1sK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgyp0rE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5G0o+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB5
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MnN29jayE5oLmtGjHj5dtA3XNK1r
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYzXRF1VBuFA
WGZ0+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c50Wna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8H0n40BYqxKy8
ZJyvfxsIPh0Na76PaBIs6ZlqA0f1LrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK1306A
KHKgfiigQZ1+gv5F1yXH
-----END CERTIFICATE-----
```

Moyen-Orient (Émirats arabes unis) – me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMakGA1UEBhMCMVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s50f2EbdSP09EAMMeP4C2USZpRV1AI1H7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdirmVClpJ+f6AR7ECLCT7up1/63xhv401fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUA12BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v60uqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFEnEj6EwoFh03zwyjMim4TwWeotUfI0o4K0uHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZ16Ae1U1ZAFM0/7PSSoDgYQAAGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWahCkyIeAydXL9AWnphK6yp10DEMBF168Xq8Hp23s0WYf8mo0hqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKOZIZjgEAwMvADAsAhQD3Z
+XGmzKmgALgGcVX/Qf1+Tn4QIUH1cgksBSVKbwj81tovBMJeKgdYo=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAzygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxZAJBgNVBAYTA1VTMRkwFwYDVQQIDDBBYXNoaW5m
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMFBAjGaa0ymRo1C3qzE4rIenmahvUp1u9ZmLwL1idwXMRX2R
+d2SeoK0KQWoc2U0FZMHYxDue7zkyk1CIRaBukTeY13/
RIr1c6X61zJ5BBtZX1HwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHUBTvJE2+WX00FTEj4hRVjameE1nEno08Z7fUVl0AFD1Do69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```



```

hhy1KHVpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDlwAwLAIUWXB1k40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAKGA1UEBhMCVVMxGTAXBgNVBAGTEFdhc2hpbmd0b24gU3RhdGUxEDA0
BgNVBACsTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBZXWlGU2Vydm1jZXMgTEExD
MB4XDTI0MDQyOTE2NDYwOVVoXDTI0MDQyODE2NDYwOVowXDELMAKGA1UEBhMCVVMx
GTAXBgNVBAGTEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBACsTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBZXWlGU2Vydm1jZXMgTEExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCChvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvP12anJ0+eIB
UqPfQG09kZ1wpWpmy08bGB2RWqWxCwUB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13h0IcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHGDAdBgNVHQ4EFgQUJdbMCBXXtvCcwWdUUIzvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXXtvCcwWdUUIzvtUF2UTihYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWV0dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAAQH/BAGwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBONarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaK009Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
-----END CERTIFICATE-----

```

RSA-2048

```

-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyox4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNTA4MTQw
ODU4MDJJaGA8yMTk1MDExNzA4NTgwM1owXDELMAKGA1UEBhMCVVMxGTAXBgNVBAGT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBACsTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBZXWlGU2Vydm1jZXMgTEExDMIIIBjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIB
CgKCAQEAW45IhGZVbQcy1fHBqzR0h08Csrdzxj/WP4cRbJo/2DAnimVrCCDs5086
FA39Zo1xsDuJHD1wMKqeXYXkJXHYbcPwC6EYYAnR+P1LG+aNS0GUzsy202S03hT0
B20hWPCqpPp39itIrH64id6nbNRJ0zLm6evHuepMAHR4/0V7hyG0iGaV/v9zqiNA
pMCLhbh2xk0P035HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRwapM290hA

```

```
cRJfJ/d/+wBTz1fkW0Z7TF+EWRIN5ITEad1DTPnF1r8kBRuDcS/1IGFwr00HLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAD
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEsBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6
b24gV2ViIFNlcnZpY2VzIEExMQ4IJAMcyox4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAC0oWSBf7b9A1cNr141r3QWwSc7k90/tUZa1
P1T0G30b12x9T/ZiBsQpbUvs01fotG0XqGVVHcIx38EbVwbw9KJGXbGSCJSEJKw
vGctc/jYMHXfhx675zmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4Njfy/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/Xm06k+Jv0eP0Gh
JzGk5t1QrSju+MqNPfK3+107o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

Chine (Beijing) – cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk10TE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEsBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6
b24gV2ViIFNlcnZpY2VzIEExMQ4IwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/1
gsw9+QSnEJeYWnmivJW0Bdn9CyDpN7cpHVmeGgNjL2fvImWyWe2f2Kq/BL917N7C
P2ZT52/sH9orlck1n2z08xPi7MIItgPHQwu30xsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAGBMatPHhRBqhwH0/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJs1Fc190TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWfa0dy0+00aECAwEAATANBgkqhkiG9w0BAQsFAA0CAQEAdSzn2+0E
V1BfR3DPWJHWRf1b7z1+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6k7G6EtqhZUqteY7
zAceoLrVu/70ynRyfqetJVGichaaxLNM31cr6kcx0owb+WQQ84cwrB3keykH4gRX
KHB2r1WSxta+2panSE01JX2q5jhcFP90rD0tZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZ1nIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+611MVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFhbQp1peGC19id0UqxPxWsasWxQX00azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```

MIIDCzCCAnSgAwIBAgIJALS0Mb0oU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExB
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6
b24gV2ViIFN1cnZpY2VzIEExMQzCBnzANBghkqhkiG9w0BAQEFAA0BjQAwYkCgYEA
uhhUN1qAZdcwWB/OSDVGk30A99EFz0n/mJlmcIQ/Xwu2dFJWmSCqEAE6gjuFCjQ
q3voxAhC2CF+e1KtJW/C0Sz/LYo60PUqd6iXF4h+upB9Hk00GuWHXsHBTsvgkgGA
1CGge14U0Cdq+23eANr8N8m28Uz1jjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR00BBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIG0BgNVHSM
eGYYwgY0AFBkZu3wT27NnYgrfH+xJz4HJaNJoWcKXjBcMQswCQYDVQQGEwJVUzEZ
MBCGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFd1YiBTZXJ2aWw1cyBMTE0CCQ0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqzm117e8Hgb
oADS0ph+YUz5P/bUCm61wFj1xaTfwKcuTR3ytj7bFLow5Bm7Sa+TC1310Gb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUEK+MRiWu+0h5/lJGii3qw4YByx
SUD1RyNy1jJFstEZj0hs
-----END CERTIFICATE-----

```

RSA-2048

```

-----BEGIN CERTIFICATE-----
MIID0zCCAi0gAwIBAgIJJA0trM5XLDsjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBhZG9uIFd1Yydm1jZXMgTExDMiIBIjANBgkqhkiG9w0BAQEFAA0CAQA8AMIIB
CgKCAQEAvBz+WQNdpM9S+aUUL0QEriTmNDUrrjLWlr7Sfa0JScBzis5D5ju0jh1
+qJdkbuGktFX50TWtm8pWhInX+hIo0S3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LM1CN9TwnRK0ToEabmDKorss4zF17VSsbQJwcBSf0cIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9Kxs0rcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh40bX1FN92VtvzD6QBs3CcoFWgyWgVzgdNG5VCbsiiuRdmii3kciZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQAAMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWyhyYIEShF1P1qDhs7F4L46/51c4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcR0115ag8d/JXGzcTCn1DXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEI0tbH1P+g5y113bI21eYE6Tm8
LKbyfK/532xJPq09abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----

```

Chine (Ningxia) – cn-northwest-1

DSA

```

-----BEGIN CERTIFICATE-----
MIIDNjCCA4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFAADBCMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFd1YiBTZXJ2aWw1cyBMTEMwIBcNMTUwNTEzMDk10TE1
WhgPMjE5NDEwMTYw0TU5MTVaMFwxZzA1BjBGNVBA1VTMRkwFwYDVQQIEExBXyXNo
aW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6b24g
V2ViIFN1cnZpY2VzIEExMQzCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/1
gsw9+QSnEJeYWnmivJW0Bdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL917N7C
P2ZT52/sH9orlck1n2z08xPi7MIItgPHQwu30xsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAGBMatPHhRBqhwH0/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJs1Fc190TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWfa0dy0+00aECAwEAATANBgkqhkiG9w0BAQsFAA0CAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7z1+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/70ynRyfQetJVGichaaxLNM31cr6kcx0owb+WQQ84cwrB3keykH4gRX
KHB2r1WSxta+2panSE01JX2q5jhcFP90rD0tZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZ1nIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+611MVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFhbQp1peGC19id0UqxPxWsasWxQX00azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDCzCCANsGawIBAgIJALS0Mb0oU2svMA0GCSqGSIb3DQEBwUAMFwxZzA1BjBGNV
BAYTA1VTMRkwFwYDVQQIEExBXyXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxZzA1BjBGNVBA1VTMRkwFwYDVQQIEExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEXdBbWF6
b24gV2ViIFN1cnZpY2VzIEExMQzCBnzANBgkqhkiG9w0BAQEFAA0BjQAwgYkCgYEA
uhhUN1qAZdcWwB/0SDVDGk30A99EFz0n/mJlmcIQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+e1KtJW/C0Sz/LYo60PUqd6iXF4h+upB9Hk00GuWHXsHBTsvgkgGA
1CGge14U0Cdq+23eANr8N8m28Uz1jjSnTlrYCHtzN4sCAwEA0B1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR00BBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIG0BgNVHSM
eGYYwgY0AFBkZu3wT27NnYgrfH+xJz4HJaNJoWcKXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFd1YiBTZXJ2aWw1cyBMTE0CCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBwUAA4GBAECji43p+oPkYqzm117e8Hgb
oADS0ph+YUz5P/bUCm61wFj1xaTfwKcuTR3ytj7bFLow5Bm7Sa+TC1310Gb2taon

```

```
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUEk+MRiWu+0h5/1JGii3qw4YByx
SUDlRyNy1jJFstEZj0hs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIID0zCCAi0gAwIBAgIJAPu4ssY3B1zcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQKIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQKHEwdTZWF0
dGx1MSAwHgYDVQKKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xNTEyMDFy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAKGA1UEBhMVCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBhXZWIgU2Vydm1jZXMgTEExMjI1IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAs0iGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWmd90qvTfiNrT6vewP813QdJ3EENZ0x4ERcf/Wd22tV72kxD
yw1Q3I10MH4b0ItGQAxU50tXCjBZEEUZoo0kU8RoUQ0U2Pq14NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJU556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKktf/CsSJ1F
w3qXqFJQA0VwsqjFyHXFI32I/G0upwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQuS8E0C0pcFJFxp2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uX1s35
qQrarczUJ9EXDhrv7VmngIk9H3YsxYr1DGEqh/oz4Ze4UL0gnfkauanHikk+BUeSg
/jTD+7e+niEzJPihHdsVKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXc0okwu6l6kfzigGkJBxkcq4gre3szZFdCQCuioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

AWS GovCloud (USA Est) — -1 us-gov-east

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgqhkiG9w0BAQ0DMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQKIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQKHEwdTZWF0dGx1MSAwHgYD
VQKKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAeFw0xMjI1MDFyMTI5MzJaGA8y
MTk1MDUwODIxMjkzMlowXDELMAKGA1UEBhMVCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDA0BgNVBAClTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBhXZWI
gU2Vydm1jZXMgTEExMjI1IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0iGi
4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9cuJPNbiy9wSA9v
lyfWmd90qvTfiNrT6vewP813QdJ3EENZ0x4ERcf/Wd22tV72kxDyw1Q3I10MH4b0I
tGQAxU50tXCjBZEEUZoo0kU8RoUQ0U2Pq14NTiUpzWacNutAn5HHS7MDc4lUlsJqbN
+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3Ap+oPbentv1qd7wvPJ
U556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKktf/CsSJ1Fw3qXqFJQA0VwsqjFyHX
FI32I/G0upwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCnUm00QHvUsJSN6KATbghow
LynHn3wZSQuS8E0C0pcFJFxp2SV0NYkERbXu0n/Vhiyq5F8v4/bRA2/xpedLWmvFs
7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uX1s35qQrarczUJ9EXDhrv7VmngIk9
H3YsxYr1DGEqh/oz4Ze4UL0gnfkauanHikk+BUeSg/jTD+7e+niEzJPihHdsVKFDlud
5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEkRLPdNse7N6UvSnuXc0okwu6l6kfzig
GkJBxkcq4gre3szZFdCQCuioj7Z4xtuTL8YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

```

hhy1KHVpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNMp9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKm11qx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDlwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qe1PCiShB1KCCj4wDQYJKoZIhvcNAQEL
BQAwXDELMAKGA1UEBhMCVVMxGTAXBgNVBAGTEFdhc2hpbmd0b24gU3RhdGUxEDA0
BgNVBAClTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBZXWVjZm1jZXMgTEExD
MB4XDTI0MDUwNzE1MjIzN1oXDTI0MDUwNzE1MjIzN1owXDELMAKGA1UEBhMCVVMx
GTAXBgNVBAGTEFdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBZXWVjZm1jZXMgTEExDMIGFMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVP9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBR09K80a1
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHGDAdBgNVHQ4EFgQU1ZXneBYnPVYXkHV1Vjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPVYXkHV1Vjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIEExBXYXNoaW50bnV0eXN1cm9udG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IULVyrqjjw
Z461qe1PCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQBfAL/YZv0y3zmVbXjyxQCsD1oeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
puIAf05x6GQiEqfBmk+YmXJfcTmJB4Ebaj4egFls1JPSHyC2xuydHlr3B04IN0H5
Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgg8zErQVQ==
-----END CERTIFICATE-----

```

RSA-2048

```

-----BEGIN CERTIFICATE-----
MIID0zCCAi0gAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIEExBXYXNoaW50bnV0eXN1cm9udG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQQKEXdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQzAgFw0xODA0MTAx
MjMyND1aGA8yMTk3MDkxMzEyMzI0VowXDELMAKGA1UEBhMCVVMxGTAXBgNVBAGTE
Fdhc2hpbmd0b24gU3RhdGUxEDA0BgNVBAClTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBZXWVjZm1jZXMgTEExDMIIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIB
CgKCAQEAv9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhw3SULoKcKmkqE61tVFrVuPT33La1UufguT9k8ZDDu09C
hQNHUdSVEuVrK3bLjaSsM0S7Uxmnn71YT990IREowvnnBNBsBlcabfQTBV04xfUG0
/m0XUiuFj0xBqbNzkEib1W7vK7ydSJtFMS1jga54UAVXibQt9EAIIF7B8k912iLa

```

```

mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7d0V1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
h02W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1LZVhB0mLshy1lh3RRoL30hp3jCwXytkWQ7E1cGjDzNGc0FArZB8xFyQNdk
MNvXDi/ErzgrHGSpcvmGHi0hMf3UzChMwbIr6udoD1MbSI07+8F+jUJkh4X111Kb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKx0bRrhU3h4JHdp1Zel1pZ61h5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrf0ds4VrVVSj+x0ZdY19P1v2
9shw5ez6Cn7E3IfzqNH0
-----END CERTIFICATE-----

```

AWS GovCloud (US-Ouest) — -1 us-gov-west

DSA

```

-----BEGIN CERTIFICATE-----
MIIC7TCCAqQCCQCWukjZ5V4aZzAJBgqhkJ00AQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEyBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQKKExdBbWF6b24gV2ViIFN1cnZpY2VzIEEMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEyBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQKKExdBbWF6b24gV2ViIFN1
cnZpY2VzIEEMQzCCAbcwggEsBgqhkJ00AQBMIIIBHwKBQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8f0Epp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLc1nd/YozqNNmgIyZecN7Eg1K9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nvwHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJ1/U
hhy1KHVpCG19fueQ2s6IL0Ca0/buyCU1CiYQk40KNHCcHfNiZbd1x1E9rpUp7bnF
lRa2v1ntMX3carVDdbtPEWmdxSCYsYFDk4mZr0LBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQ0Gx5ho8WqD+aTebS+k2tn92BBPqeZqpWRa5P/+jrdKml1qx41lHW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAKGBYqGSM44BAMDLwAwLAIUWXB1k40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----

```

RSA

```

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb71UHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBACTB1N1YXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWVzU2VydmljZXMgTEEx
MB4XDTE0MDUwNzE3MzAzM1oXDTE1MDUwNjE3MzAzM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBACTB1N1YXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWVzU2VydmljZXMgTEExDMIGfMA0GCSqGSIb3DQEBAQUA

```

```
A4GNADCBiQKBgQCpohwYUVP9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBR09K80a1
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLnrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHV1Vjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHV1Vjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdT
ZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IUe5wGF3jf
b71UHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQCbtDpx1Iob9SUrEY4exMnlwQ1mkTLyA8tYGWzchCJOJJEPfsw0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d80Wt0JQcI+ZnFfG4
KyM4rUsBr1jpG2a0Cm12iACEyrvgJJrS8VZwUDZS6mZEnn/1hA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIID0zCCAi0gAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIEExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZW
FdGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIEExMQ4IUe5wGF3jfb7
1UHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AA0BgQCbtDpx1Iob9SUrEY4exMnlwQ1mkTLyA8tYGWzchCJOJJEPfsw0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d80Wt0JQcI+ZnFfG4
KyM4rUsBr1jpG2a0Cm12iACEyrvgJJrS8VZwUDZS6mZEnn/1hA==
-----END CERTIFICATE-----
```

Rôles d'identité d'instance

Chaque instance que vous lancez est dotée d'un rôle d'identité d'instance qui représente son identité. Un rôle d'identité d'instance est un type de rôle IAM. AWS les services et fonctionnalités intégrés pour utiliser le rôle d'identité d'instance peuvent l'utiliser pour identifier l'instance auprès du service.

Les informations d'identification des rôles d'identité d'instance sont accessibles à partir du service des métadonnées d'instance (IMDS) à l'adresse `/identity-credentials/ec2/security-credentials/ec2-instance`. Les informations d'identification se composent d'une paire de clés d'accès AWS temporaires et d'un jeton de session. Ils sont utilisés pour signer les demandes AWS Sigv4 aux AWS services qui utilisent le rôle d'identité d'instance. Les informations d'identification sont présentes dans les métadonnées de l'instance, qu'un service ou une fonctionnalité utilisant les rôles d'identité d'instance soit activé ou non sur l'instance.

Les rôles d'identité d'instance sont automatiquement créés lors du lancement d'une instance, ne font l'objet d'aucun document de politique d'approbation des rôles et ne sont soumis à aucune politique d'identité ou de ressources.

Services pris en charge

Les AWS services suivants utilisent le rôle d'identité d'instance :

- Amazon EC2 — EC2 [Instance Connect](#) utilise le rôle d'identité d'instance pour mettre à jour les clés d'hôte d'une instance Linux.
- Amazon GuardDuty — [Runtime Monitoring](#) utilise le rôle d'identité de l'instance pour permettre à l'agent d'exécution d'envoyer des données télémétriques de sécurité au point de terminaison du VPC GuardDuty .
- AWS Security Token Service (AWS STS) — Les informations d'identification du rôle d'identité de l'instance peuvent être utilisées avec l' AWS STS [GetCallerIdentity](#) action.
- AWS Systems Manager— Lorsque vous utilisez [la configuration de gestion d'hôte par défaut](#), AWS Systems Manager utilise l'identité fournie par le rôle d'identité d'instance pour enregistrer les instances EC2. Après avoir identifié votre instance, Systems Manager peut transmettre votre rôle `AWSSystemsManagerDefaultEC2InstanceManagementRole` IAM à votre instance.

Les rôles d'identité d'instance ne peuvent pas être utilisés avec d'autres AWS services ou fonctionnalités car ils ne sont pas intégrés aux rôles d'identité d'instance.

ARN des rôles d'identité d'instance

L'ARN du rôle d'identité d'instance a le format suivant :

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Par exemple :

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-0123456789example
```

Pour plus d'informations sur les ARN, veuillez consulter la rubrique [Amazon Resource Names \(ARN\)](#) dans le Guide de l'utilisateur IAM.

Exécutez des commandes sur votre instance Amazon EC2 au lancement

Lorsque vous lancez une instance Amazon EC2, vous pouvez transmettre les données utilisateur à l'instance qui est utilisée pour effectuer des tâches de configuration automatisées ou pour exécuter des scripts après le démarrage de l'instance.

Si vous êtes intéressé par des scénarios d'automatisation plus complexes, vous pouvez envisager AWS CloudFormation ou AWS OpsWorks. Pour plus d'informations, consultez les ressources suivantes :

- [Déploiement d'applications sur Amazon EC2 avec AWS CloudFormation](#) dans le Guide de l'utilisateur AWS CloudFormation .
- [AWS OpsWorks Guide de l'utilisateur](#).

Sur les instances Linux, vous pouvez transmettre deux types de données utilisateur à Amazon EC2 : les scripts shell et les directives cloud-init. Vous pouvez également transmettre ces données à l'assistant de lancement d'instance sous forme de texte brut, de fichier (utile pour lancer des instances à l'aide des outils de ligne de commande) ou de texte codé en base64 (pour les appels d'API).

Sur les instances Windows, les agents de lancement gèrent vos scripts de données utilisateur. Les sections suivantes présentent les différences dans la manière dont les données utilisateur sont traitées sur chaque système d'exploitation.

Comment Amazon EC2 gère les données utilisateur pour les instances Linux

Dans les exemples suivants, les commandes du [serveur Install a LAMP sur Amazon Linux 2](#) sont converties en un script shell et en un ensemble de directives cloud-init qui s'exécutent au lancement de l'instance. Dans chaque exemple, les tâches suivantes sont exécutées par les données de l'utilisateur :

- Les packages logiciels de distribution sont mis à jour.
- Le serveur web, les packages php et mariadb nécessaires sont installés.
- Le service httpd est lancé et activé via la commande systemctl.
- L'utilisateur ec2-user est ajouté au groupe Apache.
- La propriété et les autorisations sur les fichiers appropriées sont définies pour le répertoire web et les fichiers qu'il contient.
- Une page Web simple est créée pour tester le serveur Web et le moteur PHP.

Table des matières

- [Prérequis](#)
- [Données utilisateur et scripts shell](#)
- [Données utilisateur et console](#)
- [Directives sur les données utilisateur et Cloud-Init](#)
- [Les données utilisateur et le AWS CLI](#)
- [Combiner des scripts shell et des directives cloud-init](#)

Prérequis

Les exemples de cette rubrique supposent ce qui suit :

- Votre instance possède un nom DNS public auquel on peut accéder à partir d'Internet.
- Le groupe de sécurité associé à votre instance est configuré pour autoriser le trafic SSH (port 22) afin de vous permettre de vous connecter à ladite instance pour afficher les fichiers journaux de sortie.
- Votre instance est lancée avec une AMI Amazon Linux 2. Ces instructions sont destinées à Amazon Linux 2, et il se peut que les commandes et les directives ne fonctionnent pas pour d'autres distributions Linux. Pour obtenir plus d'informations sur d'autres distributions, comme leur support pour cloud-init, consultez leur documentation spécifique.

Données utilisateur et scripts shell

Si vous connaissez le scripting de shell, il s'agit de la méthode la plus simple et la plus complète pour envoyer des instructions à une instance lors du lancement. L'ajout de ces tâches au moment

du démarrage augmente le temps que cela prend pour démarrer l'instance. Vous devriez laisser s'écouler quelques minutes supplémentaires pour que les tâches s'effectuent avant de vérifier que le script utilisateur a fini avec succès.

Important

Par défaut, les scripts de données utilisateur et les directives cloud init s'exécutent uniquement pendant le cycle de démarrage lorsque vous lancez une instance pour la première fois. Vous pouvez mettre à jour votre configuration pour vous assurer que vos scripts de données utilisateur et vos directives cloud-init s'exécutent chaque fois que vous redémarrez votre instance. Pour plus d'informations, consultez [Comment utiliser les données utilisateur pour exécuter automatiquement un script à chaque redémarrage de mon instance Linux Amazon EC2 ?](#) dans le AWS Knowledge Center.

Les scripts shell de données utilisateur doivent commencer par les caractères `#!` et le chemin vers l'interpréteur que vous avez choisi pour la lecture du script (généralement `/bin/bash`). Pour une introduction aux scripts shell, consultez le [manuel de référence Bash](#) sur le site Web du système d'exploitation GNU.

Les scripts entrés en tant que données utilisateur sont exécutés en tant qu'utilisateur root, donc n'utilisez pas la commande `sudo` dans le script. N'oubliez pas que tous les fichiers que vous créez seront la propriété de l'utilisateur root. Si vous avez besoin qu'un utilisateur non root ait accès aux fichiers, vous devez modifier les autorisations en conséquence dans le script. Par ailleurs, étant donné que le script n'est pas exécuté de façon interactive, vous ne pouvez pas inclure des commandes qui nécessitent les réactions de l'utilisateur (comme `yum update` sans l'indicateur `-y`).

Si vous utilisez une AWS API, y compris la AWS CLI, dans un script de données utilisateur, vous devez utiliser un profil d'instance lors du lancement de l'instance. Un profil d'instance fournit les AWS informations d'identification appropriées requises par le script de données utilisateur pour émettre l'appel d'API. Pour plus d'informations, consultez [Utilisation de profils d'instance](#) dans le IAM Guide de l'utilisateur. Les autorisations que vous attribuez au rôle IAM dépendent des services que vous appelez avec l'API. Pour plus d'informations, consultez [Rôles IAM pour Amazon EC2](#).

Le fichier journal de sortie cloud-init (`/var/log/cloud-init-output.log`) capture la sortie de la console, si bien que vous pouvez facilement déboguer vos scripts après un lancement si l'instance ne se comporte pas comme vous le vouliez. Pour afficher le fichier journal, [connexion à l'instance](#) et ouvrez `/var/log/cloud-init-output.log`.

Lorsqu'un script de données utilisateur est traité, il est copié dans et exécuté à partir de `/var/lib/cloud/instances/instance-id/`. Le script n'est pas supprimé après son exécution. Veillez à supprimer les scripts de données utilisateur dans `/var/lib/cloud/instances/instance-id/` avant de créer une AMI à partir de l'instance. Dans le cas contraire, le script figurera dans ce répertoire sur toute instance lancée à partir de l'AMI.

Données utilisateur et console

Vous pouvez spécifier des données utilisateur d'instance lorsque vous lancez l'instance. Si le volume racine de l'instance est un volume EBS, vous pouvez également arrêter l'instance et mettre à jour ses données utilisateur.

Spécification des données utilisateur d'instance au moment du lancement

Suivez la procédure pour [lancer une instance](#). Le champ User data (Données utilisateur) se trouve dans la section [Détails avancés](#) de l'assistant de lancement d'instance. Saisissez votre script shell dans le champ User data (Données utilisateur), puis terminez la procédure de lancement de l'instance.

Dans l'exemple de script ci-dessous, le script crée et configure notre serveur web.

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Laissez assez de temps à l'instance pour lancer et exécuter les commandes dans votre script, puis vérifiez que votre script a terminé les tâches que vous souhaitez.

Pour notre exemple, dans un navigateur web, saisissez l'URL du fichier test PHP que le script a créé. Cette URL est l'adresse DNS publique de votre instance suivie par une barre oblique et le nom du fichier.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Vous devriez voir la page d'informations PHP. Si vous ne pouvez pas voir la page d'informations PHP, vérifiez que le groupe de sécurité que vous utilisez contient une règle pour permettre le trafic HTTP (port 80). Pour plus d'informations, consultez [Ajouter des règles à un groupe de sécurité](#).

(Facultatif) Si votre script n'a pas accompli les tâches que vous attendiez ou si vous voulez uniquement vérifier que votre script s'est terminé sans erreur, [connectez-vous à l'instance](#), examinez le fichier journal de sortie cloud-init (`/var/log/cloud-init-output.log`) et recherchez les messages erronés dans les résultats.

Pour obtenir des informations supplémentaires sur le débogage, vous pouvez créer une archive Mime en plusieurs parties qui comporte la section de données cloud-init avec la directive suivante :

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Cette directive envoie la sortie de la commande de votre script à `/var/log/cloud-init-output.log`. Pour plus d'informations sur les formats de données cloud-init et la création d'archives Mime en plusieurs parties, consultez [Formats de cloud-init](#).

Affichage et mise à jour des données utilisateur d'instance

Pour mettre à jour les données de l'utilisateur de l'instance, vous devez d'abord arrêter l'instance. Si l'instance est en cours d'exécution, vous pouvez afficher les données utilisateur, mais vous ne pouvez pas les modifier.

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

Pour modifier les données utilisateur d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.

3. Sélectionnez l'instance et choisissez État de l'instance, Arrêter l'instance. Si cette option est désactivée, l'instance est déjà arrêtée ou son périphérique racine est un volume de stockage d'instances.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter. L'arrêt de l'instance peut prendre quelques minutes.
5. Alors que l'instance est toujours sélectionnée, choisissez Actions, Instance settings (Paramètres de l'instance), Edit user data (Modifier les données utilisateur).
6. Modifiez les données utilisateur selon vos besoins, puis choisissez Save (Enregistrer).
7. Démarrez l'instance. Les nouvelles données utilisateur sont visibles sur votre instance, après son démarrage. Par contre, les scripts des données utilisateur ne sont pas exécutés.

Directives sur les données utilisateur et Cloud-Init

Le package cloud-init configure les aspects spécifiques d'une nouvelle instance Amazon Linux lorsqu'elle est lancée. Il configure plus particulièrement le fichier `.ssh/authorized_keys` pour l'utilisateur `ec2` afin que vous puissiez vous connecter avec votre clé privée. Pour plus d'informations sur les tâches de configuration effectuées par le package cloud-init pour les instances Amazon Linux, consultez la section [Utilisation de cloud-init sur Amazon Linux 2](#) dans le guide de l'utilisateur Amazon Linux 2.

Les directives d'utilisateur cloud-init peuvent être transférées vers une instance au moment du lancement tout comme un script, même si la syntaxe est différente. Pour plus d'informations sur cloud-init, consultez <http://cloudinit.readthedocs.org/en/latest/index.html>.

Important

Par défaut, les scripts de données utilisateur et les directives cloud init s'exécutent uniquement pendant le cycle de démarrage lorsque vous lancez une instance pour la première fois. Vous pouvez mettre à jour votre configuration pour vous assurer que vos scripts de données utilisateur et vos directives cloud-init s'exécutent chaque fois que vous redémarrez votre instance. Pour plus d'informations, consultez [Comment utiliser les données utilisateur pour exécuter automatiquement un script à chaque redémarrage de mon instance Linux Amazon EC2 ?](#) dans le AWS Knowledge Center.

L'ajout de ces tâches au moment du démarrage augmente le temps que cela prend pour démarrer une instance. Vous devriez laisser s'écouler quelques minutes supplémentaires pour que les tâches s'effectuent avant de vérifier que vos directives sur les données utilisateur sont terminées.

Pour transférer les directives cloud-init vers une instance avec les données utilisateur

1. Suivez la procédure pour [lancer une instance](#). Le champ User data (Données utilisateur) se trouve dans la section [Détails avancés](#) de l'assistant de lancement d'instance. Saisissez le texte de la directive cloud-init dans le champ User data (Données utilisateur), puis terminez la procédure de lancement de l'instance.

Pour l'exemple ci-dessous, les directives créent et configurent un serveur Web sur Amazon Linux

2. La ligne `#cloud-config` en haut est requise pour identifier les commandes en tant que directives cloud-init.

```
#cloud-config
repo_update: true
repo_upgrade: all

packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- sudo systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

2. Laissez assez de temps à l'instance pour lancer et exécuter les directives dans vos données utilisateur, puis vérifiez que vos directives ont terminé les tâches que vous souhaitez.

Pour notre exemple, dans un navigateur Web, saisissez l'URL du fichier test PHP que les directives ont créé. Cette URL est l'adresse DNS publique de votre instance suivie par une barre oblique et le nom du fichier.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Vous devriez voir la page d'informations PHP. Si vous ne pouvez pas voir la page d'informations PHP, vérifiez que le groupe de sécurité que vous utilisez contient une règle pour permettre le trafic HTTP (port 80). Pour plus d'informations, consultez [Ajouter des règles à un groupe de sécurité](#).

3. (Facultatif) Si vos directives n'ont pas accompli les tâches que vous attendiez ou si vous voulez uniquement vérifier que vos directives se sont terminées sans erreur, [connectez-vous à l'instance](#), examinez le fichier journal de sortie (`/var/log/cloud-init-output.log`) et recherchez les messages erronés dans les résultats. Pour plus d'informations sur le débogage, vous pouvez ajouter la ligne suivante à vos directives :

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Cette directive envoie le résultat `runcmd` à `/var/log/cloud-init-output.log`.

Les données utilisateur et le AWS CLI

Vous pouvez utiliser le AWS CLI pour spécifier, modifier et afficher les données utilisateur de votre instance. Pour plus d'informations sur l'affichage des données utilisateur de votre instance à l'aide des métadonnées d'instance, consultez [Récupération des données utilisateur d'instance depuis votre instance](#).

Sous Windows, vous pouvez utiliser le AWS Tools for Windows PowerShell au lieu du AWS CLI. Pour plus d'informations, consultez [Les données utilisateur et les outils pour Windows PowerShell](#).

Exemple : spécification des données utilisateur au moment du lancement

Pour spécifier les données utilisateur lorsque vous lancez l'instance, utilisez la commande [run-instances](#) avec le paramètre `--user-data`. Avec `run-instances`, il AWS CLI effectue le codage base64 des données utilisateur pour vous.

L'exemple suivant montre comment définir un script en tant que chaîne sur la ligne de commande :

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \  
  --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \  
  --user-data echo user data
```

L'exemple suivant montre comment définir un script en utilisant un fichier texte. Assurez-vous d'utiliser le préfixe `file://` pour spécifier le fichier.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \  
--key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \  
--user-data file://my_script.txt
```

L'exemple suivant est celui d'un fichier texte avec un script shell.

```
#!/bin/bash  
yum update -y  
service httpd start  
chkconfig httpd on
```

Exemple : Modification des données utilisateur d'une instance arrêtée

Vous pouvez modifier les données utilisateur d'une instance arrêtée à l'aide de la commande [modify-instance-attribute](#). Avec `modify-instance-attribute`, le AWS CLI n'effectue pas le codage base64 des données utilisateur pour vous.

- Sur un ordinateur Linux utilisez la commande `base64` pour encoder les données utilisateur.

```
base64 my_script.txt >my_script_base64.txt
```

- Sur un ordinateur Windows, utilisez la commande `certutil` pour encoder les données utilisateur. Avant de pouvoir utiliser ce fichier avec le AWS CLI, vous devez supprimer la première ligne (CERTIFICAT DE DÉBUT) et la dernière (CERTIFICAT DE FIN).

```
certutil -encode my_script.txt my_script_base64.txt  
notepad my_script_base64.txt
```

Utilisez les paramètres `--attribute` et `--value` afin d'utiliser le fichier texte encodé pour spécifier les données utilisateur. Assurez-vous d'utiliser le préfixe `file://` pour spécifier le fichier.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute  
userData --value file://my_script_base64.txt
```

Exemple : Effacer les données utilisateur d'une instance arrêtée

Pour supprimer les données utilisateur existantes, utilisez la commande [modify-instance-attribute](#) comme suit :

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Exemple : Affichage des données utilisateur

Pour extraire les données utilisateur pour une instance, utilisez la commande [describe-instance-attribute](#). Avec `describe-instance-attribute`, le AWS CLI n'effectue pas de décodage base64 des données utilisateur pour vous.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute  
userData
```

Voici un exemple de sortie avec les données utilisateur base64 encodées.

```
{  
  "UserData": {  
    "Value":  
    "IyEvYm1uL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHNoYXJ0CmNoa2NvbmZpZyBodHRwZCBvbG=="  
  },  
  "InstanceId": "i-1234567890abcdef0"  
}
```

- Sur un ordinateur Linux, utilisez l'option `--query` pour obtenir les données utilisateur encodées et la commande `base64` pour les décodés.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute  
userData --output text --query "UserData.Value" | base64 --decode
```

- Sur un ordinateur Windows, utilisez l'option `--query` pour obtenir les données utilisateur codées et la commande `certutil` pour les décodés. Notez que la sortie encodée est stockée dans un fichier et que la sortie décodée est stockée dans un autre fichier.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute  
userData --output text --query "UserData.Value" >my_output.txt  
certutil -decode my_output.txt my_output_decoded.txt  
type my_output_decoded.txt
```

Voici un exemple de sortie.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Combiner des scripts shell et des directives cloud-init

Par défaut, vous ne pouvez inclure qu'un seul type de contenu à la fois dans les données utilisateur. Toutefois, vous pouvez utiliser les types de contenu `text/cloud-config` et `text/x-shellscript` dans un fichier MIME en plusieurs parties pour inclure à la fois un script shell et des directives cloud-init dans vos données utilisateur.

Le format MIME en plusieurs parties est représenté ci-dessous.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
cloud-init directives

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
shell script commands
--/--
```

Par exemple, les données utilisateur suivantes incluent des directives cloud-init et un script shell bash. Les directives cloud-init créent un fichier (`/test-cloudinit/cloud-init.txt`) et y écrivent `Created by cloud-init`. Le script shell bash crée un fichier (`/test-userscript/userscript.txt`) et y écrit `Created by bash shell script`.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
runcmd:
- [ mkdir, /test-cloudinit ]
write_files:
- path: /test-cloudinit/cloud-init.txt
  content: Created by cloud-init

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
mkdir test-userscript
touch /test-userscript/userscript.txt
echo "Created by bash shell script" >> /test-userscript/userscript.txt
--//--
```

Comment Amazon EC2 gère les données utilisateur pour les instances Windows

Sur les instances Windows, les agents de lancement par défaut de la version de votre système d'exploitation gèrent les données utilisateur comme suit.

- [EC2Launch v2](#) exécute des scripts de données utilisateur sur Windows Server 2022
- [???](#) exécute des scripts de données utilisateur sur Windows Server 2016 et 2019
- [???](#) exécute des scripts de données utilisateur sur les versions de Windows Server antérieures à Windows Server 2016

Pour des exemples d'assemblage d'une UserData propriété dans un AWS CloudFormation modèle, voir Propriété codée en [Base64 et UserData Propriété codée en Base64 avec AccessKey](#) et. UserData SecretKey

Pour un exemple d'exécution de commandes sur une instance au sein d'un groupe Auto Scaling qui fonctionne avec des hooks de cycle de vie, consultez [Tutoriel : Configurer les données utilisateur pour récupérer l'état du cycle de vie cible via les métadonnées de l'instance](#) dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

Table des matières

- [Scripts de données utilisateur](#)
- [Exécution de données utilisateur](#)
- [Données utilisateur et console](#)
- [Les données utilisateur et les outils pour Windows PowerShell](#)

Scripts de données utilisateur

Pour EC2Config ou EC2Launch pour exécuter des scripts, vous devez placer le script dans une balise spéciale lorsque vous l'ajoutez aux données utilisateur. La balise que vous utilisez varie selon que les commandes sont exécutées dans une fenêtre d'invite de commandes (commandes par lots) ou qu'elles utilisent WindowsPowerShell.

Si vous spécifiez à la fois un script batch et un PowerShell script Windows, le script batch s'exécute en premier et le PowerShell script Windows s'exécute ensuite, quel que soit l'ordre dans lequel ils apparaissent dans les données utilisateur de l'instance.

Si vous utilisez une AWS API, y compris le AWS CLI, dans un script de données utilisateur, vous devez utiliser un profil d'instance lors du lancement de l'instance. Un profil d'instance fournit les AWS informations d'identification appropriées requises par le script de données utilisateur pour effectuer l'appel d'API. Pour plus d'informations, consultez [Profils d'instance](#). Les autorisations que vous attribuez au rôle IAM dépendent des services que vous appelez avec l'API. Pour plus d'informations, consultez [Rôles IAM pour Amazon EC2](#).

Type de script

- [Syntaxe des scripts par lots](#)
- [Syntaxe des PowerShell scripts Windows](#)
- [Syntaxe pour les scripts de configuration YAML](#)

- [Encodage Base64](#)

Syntaxe des scripts par lots

Spécifiez un script par lots à l'aide de la balise `script`. Séparez les commandes à l'aide de sauts de ligne, comme indiqué dans l'exemple suivant.

```
<script>
echo Current date and time >> %SystemRoot%\Temp\test.log
echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

Par défaut, les scripts de données utilisateur s'exécutent une seule fois, lorsque vous lancez l'instance. Pour exécuter des scripts de données utilisateur chaque fois que vous redémarrez ou démarrez l'instance, ajoutez `<persist>>true</persist>` aux données utilisateur.

```
<script>
echo Current date and time >> %SystemRoot%\Temp\test.log
echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<persist>true</persist>
```

Agent EC2Launch v2

Pour exécuter un script de données utilisateur XML en tant que processus détaché avec la tâche `executeScript EC2Launch v2` dans l'étape `UserData`, ajoutez la balise suivante à vos données utilisateur.

```
<detach>true</detach>
```

Note

La balise `detach` n'est pas prise en charge sur les agents de lancement précédents.

```
<script>
echo Current date and time >> %SystemRoot%\Temp\test.log
echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

```
<detach>true</detach>
```

Syntaxe des PowerShell scripts Windows

Les AMI AWS Windows incluent les [AWS Tools for Windows PowerShell](#). Vous pouvez donc spécifier ces applets de commande dans les données utilisateur. Si vous associez un rôle IAM à votre instance, vous n'avez pas besoin de spécifier les informations d'identification pour les applets de commande, car les applications qui s'exécutent sur l'instance utilisent les informations d'identification du rôle pour accéder aux AWS ressources (par exemple, les compartiments Amazon S3).

Spécifiez un PowerShell script Windows à l'aide de la `<powershell>` balise. Séparez les commandes à l'aide de sauts de ligne. La balise `<powershell>` est sensible à la casse.

Par exemple :

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
```

Par défaut, les scripts de données utilisateur s'exécutent une seule fois lorsque vous lancez l'instance. Pour exécuter des scripts de données utilisateur chaque fois que vous redémarrez ou démarrez l'instance, ajoutez `<persist>true</persist>` aux données utilisateur.

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Vous pouvez spécifier un ou plusieurs PowerShell arguments à l'aide de la `<powershellArguments>` balise. Si aucun argument n'est transmis, EC2Launch et EC2Launch v2 ajoutent l'argument suivant par défaut : `-ExecutionPolicy Unrestricted`

Exemple :

```
<powershell>
$file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
```

```
</powershell>  
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</  
powershellArguments>
```

Agent EC2Launch v2

Pour exécuter un script de données utilisateur XML en tant que processus détaché avec la tâche `executeScript` EC2Launch v2 dans l'étape `UserData`, ajoutez la balise suivante à vos données utilisateur.

```
<detach>true</detach>
```

Note

La balise `detach` n'est pas prise en charge sur les agents de lancement précédents.

```
<powershell>  
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")  
New-Item $file -ItemType file  
</powershell>  
<detach>true</detach>
```

Syntaxe pour les scripts de configuration YAML

Si vous utilisez EC2Launch v2 pour exécuter des scripts, vous pouvez utiliser le format YAML. Pour afficher les tâches de configuration, les détails et les exemples pour EC2Launch v2, consultez [Configuration de tâche EC2Launch v2](#).

Spécifiez un script YAML avec la tâche `executeScript`.

Exemple de syntaxe YAML pour exécuter un script PowerShell

```
version: 1.0  
tasks:  
- task: executeScript  
  inputs:  
  - frequency: always  
    type: powershell  
    runAs: localSystem
```

```
content: |-
  $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
```

Exemple de syntaxe YAML pour exécuter un script Batch

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: batch
    runAs: localSystem
  content: |-
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Encodage Base64

Si vous utilisez l'API Amazon EC2 ou un outil qui n'effectue pas l'encodage base64 des données utilisateur, vous devez encoder les données utilisateur. Si ce n'est pas le cas, une erreur indiquant qu'aucune balise script ou powershell à exécuter n'a été trouvée est consignée. Voici un exemple d'encodage à l'aide de Windows PowerShell.

```
$UserData =
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Voici un exemple de décodage à l'aide PowerShell de.

```
$Script =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Pour plus d'informations sur l'encodage base64, consultez <https://www.ietf.org/rfc/rfc4648.txt>.

Exécution de données utilisateur

Par défaut, l'exécution des données utilisateur est activée pour toutes les AMI AWS Windows lors du lancement initial. Vous pouvez spécifier que les scripts de données utilisateur doivent être exécutés au prochain réamorçage ou redémarrage de l'instance. Vous pouvez également spécifier que les

scripts de données utilisateur doivent être exécutés chaque fois que l'instance est réamorcée ou redémarre.

Note

Les données utilisateur ne sont pas activées pour être exécutées par défaut après le lancement initial. Pour activer l'exécution des données utilisateur lorsque vous redémarrez ou démarrez l'instance, consultez [Réamorçages ou démarrages suivants](#).

Les scripts de données utilisateur sont exécutés depuis le compte de l'administrateur local quand un mot de passe aléatoire est généré. Sinon, les scripts de données utilisateur sont exécutés depuis le compte système.

Lancement d'une instance

Les scripts figurant dans les données utilisateur d'instance sont exécutés lors du lancement initial de l'instance. Si la balise `persist` est trouvée, l'exécution des données utilisateur est activée pour les réamorçages ou démarrages suivants. Les fichiers journaux pour EC2Launch v2, EC2Launch et EC2Config contiennent les résultats de sortie standard ainsi que les flux d'erreurs standard.

EC2Launch v2

Le fichier journal de EC2Launch v2 est `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

Note

Le dossier `C:\ProgramData` peut être masqué. Pour afficher le dossier, vous devez afficher les fichiers et les dossiers masqués.

Les informations suivantes sont enregistrées lorsque les données utilisateur sont exécutées :

- `Info: Converting user-data to yaml format` – Si les données utilisateur ont été fournies au format XML
- `Info: Initialize user-data state` – Début de l'exécution des données utilisateur
- `Info: Frequency is: always` – Si la tâche de données utilisateur est en cours d'exécution à chaque démarrage

- **Info:** `Frequency is: once` – Si la tâche de données utilisateur est exécutée une seule fois
- **Stage:** `postReadyUserData execution completed` – Fin de l'exécution des données utilisateur

EC2Launch

Le fichier journal pour EC2Launch est `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

Le dossier `C:\ProgramData` peut être masqué. Pour afficher le dossier, vous devez afficher les fichiers et les dossiers masqués.

Les informations suivantes sont enregistrées lorsque les données utilisateur sont exécutées :

- `Userdata execution begins` – Début de l'exécution des données utilisateur
- `<persist> tag was provided: true` – Si l'identification persist est trouvée
- `Running userdata on every boot` – Si l'identification persist est trouvée
- `<powershell> tag was provided.. running powershell content` – Si la balise powershell est trouvée
- `<script> tag was provided.. running script content` – Si l'identification script est trouvée
- `Message: The output from user scripts` – Si des scripts de données utilisateur sont exécutés, leur sortie est journalisée

EC2Config

Le fichier journal pour EC2Config est `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log`. Les informations suivantes sont enregistrées lorsque les données utilisateur sont exécutées :

- `Ec2HandleUserData: Message: Start running user scripts` – Début de l'exécution des données utilisateur
- `Ec2HandleUserData: Message: Re-enabled userdata execution` – Si l'identification persist est trouvée
- `Ec2HandleUserData: Message: Could not find <persist> and </persist>` – Si la balise persist n'est pas trouvée

- `Ec2HandleUserData: Message: The output from user scripts` – Si des scripts de données utilisateur sont exécutés, leur sortie est journalisée

Réamorçages ou démarrages suivants

Lorsque vous mettez à jour des données utilisateur d'instance, les scripts de données utilisateur sont exécutés automatiquement lorsque vous redémarrez ou démarrez l'instance. Toutefois, vous pouvez activer l'exécution des données utilisateur pour que les scripts de données utilisateur soient exécutés une seule fois lorsque vous redémarrez ou démarrez l'instance ou chaque fois que vous redémarrez ou démarrez l'instance.

Si vous choisissez l'option Arrêter avec Sysprep, les scripts de données utilisateur sont exécutés quand l'instance est redémarrée ou démarrée, même si vous n'avez pas activé l'exécution des données utilisateur pour les redémarrages ou démarrages suivants. Les scripts de données utilisateur ne seront pas exécutés lors des redémarrages ou démarrages ultérieurs.

Pour activer l'exécution des données utilisateur avec EC2Launch v2 (AMI d'aperçu)

- Pour exécuter une tâche dans les données utilisateur au premier démarrage, définissez `frequency` sur `once`.
- Pour exécuter une tâche dans les données utilisateur à chaque démarrage, définissez `frequency` sur `always`.

Pour activer l'exécution des données utilisateur avec EC2Launch (Windows Server 2016 ou version ultérieure)

1. Connectez-vous à votre instance Windows.
2. Ouvrez une fenêtre de PowerShell commande et exécutez la commande suivante :

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

3. Déconnectez-vous de votre instance Windows. Pour exécuter les scripts mis à jour au démarrage suivant de l'instance, arrêtez l'instance et mettez à jour les données utilisateur.

Pour activer l'exécution des données utilisateur avec EC2Config (Windows Server 2012 R2 et versions antérieures)

1. Connectez-vous à votre instance Windows.

2. Ouvrir C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe.
3. Pour les données utilisateur, sélectionnez Activer UserData l'exécution pour le prochain démarrage du service.
4. Déconnectez-vous de votre instance Windows. Pour exécuter les scripts mis à jour au démarrage suivant de l'instance, arrêtez l'instance et mettez à jour les données utilisateur.

Données utilisateur et console

Vous pouvez spécifier des données utilisateur d'instance lorsque vous lancez l'instance. Si le volume racine de l'instance est un volume EBS, vous pouvez également arrêter l'instance et mettre à jour ses données utilisateur.

Spécification des données utilisateur d'instance au moment du lancement

Suivez la procédure pour [lancer une instance](#). Le champ User data (Données utilisateur) se trouve dans la section [Détails avancés](#) de l'assistant de lancement d'instance. Entrez votre PowerShell script dans le champ Données utilisateur, puis terminez la procédure de lancement de l'instance.

Dans la capture d'écran suivante du champ Données utilisateur, l'exemple de script crée un fichier dans le dossier temporaire Windows, en utilisant la date et l'heure actuelles dans le nom de fichier. Lorsque vous incluez `<persist>true</persist>`, le script est exécuté chaque fois que vous redémarrez ou démarrez l'instance. Si vous laissez la case Les données utilisateur ont déjà été encodées en base64 vide, la console Amazon EC2 effectue l'encodage en base64 pour vous.

User data - optional [Info](#)

Enter user data in the field.

```
<powershell>
$file = $env:SystemRoot+"\Temp\"+(Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

User data has already been base64 encoded

Affichage et mise à jour des données utilisateur d'instance

Vous pouvez afficher les données utilisateur d'instance pour n'importe quelle instance, et vous pouvez mettre à jour les données utilisateur d'instance pour une instance arrêtée.

Pour mettre à jour les données utilisateur pour une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance et choisissez Actions, État de l'instance, Arrêter l'instance.

⚠ Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Lorsque vous êtes invité à confirmer l'opération, choisissez Arrêter. L'arrêt de l'instance peut prendre quelques minutes.
5. Alors que l'instance est toujours sélectionnée, choisissez Actions, Instance settings (Paramètres de l'instance), Edit user data (Modifier les données utilisateur). Vous ne pouvez changer les données utilisateur si l'instance est en cours d'exécution, mais vous pouvez les voir.
6. Dans la boîte de dialogue Modifier les données utilisateur, mettez à jour les données utilisateur, puis cliquez sur Enregistrer. Pour exécuter des scripts de données utilisateur chaque fois que vous redémarrez ou démarrez l'instance, ajoutez `<persist>>true</persist>`, comme illustré dans l'exemple suivant.

Edit user data Info

Instance ID

 i-0655799f982552ec9

Current user data

User data currently associated with this instance

```
<powershell>
$file = $env:SystemRoot+"\Temp\"+(Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
```

 Copy user data

New user data

This user data will replace the current user data

Modify user data as text
Add your user data below

Modify user data by importing a file
Description of importing a file and what will happen to it

```
<powershell>
$file = $env:SystemRoot+"\Temp\"+(Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>>true</persist>
```

Input is already base64-encoded

Cancel

Save

7. Démarrez l'instance. Si vous avez activé l'exécution des données utilisateur pour les redémarrages ou démarrages suivants, les scripts de données utilisateur mis à jour sont exécutés dans le cadre du processus de démarrage de l'instance.

Les données utilisateur et les outils pour Windows PowerShell

Vous pouvez utiliser les Outils pour Windows PowerShell pour spécifier, modifier et afficher les données utilisateur de votre instance. Pour plus d'informations sur l'affichage des données utilisateur de votre instance à l'aide des métadonnées d'instance, consultez [Récupération des données utilisateur d'instance depuis votre instance](#). Pour plus d'informations sur les données utilisateur et le AWS CLI, voir [Les données utilisateur et le AWS CLI](#).

Exemple : Spécification des données utilisateur d'instance au moment du lancement

Créez un fichier texte avec les données utilisateur d'instance. Pour exécuter des scripts de données utilisateur chaque fois que vous redémarrez ou démarrez l'instance, ajoutez `<persist>>true</persist>`, comme illustré dans l'exemple suivant.

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>>true</persist>
```

Pour spécifier les données utilisateur de l'instance lorsque vous lancez votre instance, utilisez la [New-EC2Instance](#) commande. Cette commande n'effectue pas l'encodage base64 des données utilisateur pour vous. Utilisez les commandes suivantes pour encoder les données utilisateur dans un fichier texte nommé `script.txt`.

```
PS C:\> $Script = Get-Content -Raw script.txt
PS C:\> $UserData =
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Utilisez le paramètre `-UserData` pour transmettre les données utilisateur à la commande `New-EC2Instance`.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
-KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
-UserData $UserData
```

Exemple : Mise à jour des données utilisateur d'instance pour une instance arrêtée

Vous pouvez modifier les données utilisateur d'une instance arrêtée à l'aide de la [Edit-EC2InstanceAttribute](#) commande.

Créez un fichier texte contenant le nouveau script. Utilisez les commandes suivantes pour encoder les données utilisateur dans le fichier texte nommé `new-script.txt`.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
PS C:\> $NewUserData =
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Utilisez les paramètres `-UserData` et `-Value` pour spécifier les données utilisateur.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Exemple : Affichage des données utilisateur d'instance

Pour récupérer les données utilisateur d'une instance, utilisez la [Get-EC2InstanceAttribute](#) commande.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
userData).UserData
```

Voici un exemple de sortie. Notez que les données utilisateur sont encodées.

```
PHBvd2Vyc2h1bGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLlU51d05hbWUgdXN1ci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Utilisez les commandes suivantes pour stocker les données utilisateur encodées dans une variable, puis les décoder.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
PS C:
> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded))
```

Voici un exemple de sortie.

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
```

```
New-Item $file -ItemType file
</powershell>
<persist>>true</persist>
```

Exemple : Attribution d'un nouveau nom à l'instance pour correspondre à la valeur de la balise

Vous pouvez utiliser la [Get-EC2Tag](#) commande pour lire la valeur de la balise, renommer l'instance au premier démarrage pour qu'elle corresponde à la valeur de la balise, puis redémarrer. Pour exécuter cette commande avec succès, vous devez avoir un rôle avec les autorisations `ec2:DescribeTags` attachées à l'instance, car les informations sur les identifications sont extraites par l'appel d'API. Pour plus d'informations sur les autorisations de configuration à l'aide des rôles IAM, consultez [Attacher un rôle IAM à une instance](#).

Note

Le script échoue avec les versions Windows Server antérieures à 2008.

```
<powershell>
$instanceId = (invoke-webrequest http://169.254.169.254/latest/meta-data/instance-id -
UseBasicParsing).content
$nameValue = (get-ec2tag -filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
$pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
#Verify Name Value satisfies best practices for Windows hostnames
If ($nameValue -match $pattern)
    {Try
        {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
    Catch
        {$ErrorMessage = $_.Exception.Message
        Write-Output "Rename failed: $ErrorMessage"}}
Else
    {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Vous pouvez également renommer l'instance à l'aide d'identifications dans les métadonnées d'instance si votre instance est configurée pour accéder aux identifications à partir des métadonnées d'instance. Pour plus d'informations, consultez [Utiliser les identifications d'instance dans les métadonnées d'instance](#).

Note

Le script échoue avec les versions Windows Server antérieures à 2008.

```
<powershell>
$nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
$pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
#Verify Name Value satisfies best practices for Windows hostnames
If ($nameValue -match $pattern)
    {Try
        {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
    Catch
        {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
Else
    {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Connectez-vous à votre instance EC2

Cette section du guide de l'utilisateur Amazon EC2 fournit des informations qui vous aideront à vous connecter à votre instance Amazon EC2 après son lancement. Il fournit également des informations pour vous aider à connecter votre instance à une autre AWS ressource.

Rubriques

- [Connectez-vous à votre instance Linux](#)
- [Connexion à votre instance Windows](#)
- [Connexion à l'aide du Gestionnaire de session](#)
- [Connectez-vous à vos instances à l'aide du point de terminaison EC2 Instance Connect](#)
- [Connexion de votre instance EC2 à une ressource AWS](#)

Connectez-vous à votre instance Linux

Il existe de nombreuses façons de vous connecter à une instance Linux. Certaines varient en fonction du système d'exploitation de l'ordinateur local à partir duquel vous vous connectez. D'autres, comme

EC2 Instance Connect ou le Gestionnaire de session AWS Systems Manager , ne varient pas. Dans cette section, vous découvrirez comment vous connecter à votre instance Linux et transférer des fichiers entre votre ordinateur local et votre instance.

Avant de vous connecter à votre instance Linux, remplissez les prérequis suivants.

- [Obtenez des informations sur votre instance](#)
- [Localisation de la clé privée et définition des autorisations](#)
- [\(Facultatif\) Obtenez l'empreinte digitale de l'instance](#)

Choisissez ensuite l'une des options suivantes pour vous connecter à votre instance Linux.

Options de connexion en fonction de votre système d'exploitation local

- [Connexion à partir d'une machine locale Linux ou macOS à l'aide de SSH](#)
- [Connexion à partir d'une machine locale Windows](#)

Options de connexion depuis n'importe quel système d'exploitation local

- [Connexion à l'aide du Gestionnaire de session](#)
- [Connexion à votre instance Linux avec EC2 Instance Connect.](#)

Note

Pour obtenir des conseils de résolution des problèmes de connexion aux instances, veuillez consulter la rubrique [Résoudre les problèmes de connexion à votre instance Linux](#).

Pour résoudre les problèmes de démarrage, de configuration réseau et d'autres problèmes liés aux instances basées sur [AWS Nitro System](#), vous pouvez utiliser la [Console série EC2 pour instances Amazon EC2](#).

Obtenez des informations sur votre instance

Pour préparer la connexion à une instance, obtenez les informations suivantes à partir de la console Amazon EC2 ou en utilisant l' AWS CLI.

The screenshot shows the Amazon EC2 console interface. At the top, there's a notification 'Successfully started i-...' and a 'Launch Instances' button. Below is a table of instances with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. The 'Instance ID' column is circled in red. Below the table, the 'Instance: i-05...' details are shown. The 'Details' tab is selected and circled in red. In the 'Instance summary' section, the 'Instance ID' and 'IPv6 address' fields are circled in red. In the 'Public IPv4 DNS' field, the value 'ec2-...compute-1.amazonaws.com | open address' is circled in red.

- Obtenez le nom du serveur DNS public de l'instance.

Vous pouvez obtenir l'adresse du serveur DNS public de votre instance à partir de la console Amazon EC2. Consultez la colonne DNS IPv4 public du volet Instances. Si la colonne est masquée, choisissez l'icône des paramètres (



) dans le coin supérieur droit de l'écran et sélectionnez DNS public (IPv4). Vous pouvez également trouver le DNS public dans la section Informations sur l'instance du volet Instances. Lorsque vous sélectionnez l'instance dans le volet Instances de la console Amazon EC2, les informations relatives à cette instance apparaissent dans la partie inférieure de la page. Dans l'onglet Détails, recherchez le DNS IPv4 public.

Si vous préférez, vous pouvez utiliser les commandes [describe-instances](#) (AWS CLI) ou [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).

Si aucun DNS IPv4 public n'est affiché, vérifiez que l'état de l'instance est en cours d'exécution et que vous n'avez pas lancé l'instance dans un sous-réseau privé. Si vous avez lancé votre instance à l'aide de l'[assistant de lancement d'instance](#), vous avez peut-être modifié le champ Attribuer automatiquement une adresse IP publique sous Paramètres réseau et changé la valeur

sur Désactiver. Si vous désactivez l'option Attribuer automatiquement une adresse IP publique, aucune adresse IP publique n'est attribuée à l'instance lors de son lancement.

- (IPv6 uniquement) Obtenez l'adresse IPv6 de l'instance.

Si vous avez attribué une adresse IPv6 à votre instance, vous pouvez éventuellement vous connecter à l'instance à l'aide de son adresse IPv6 au lieu d'une adresse IPv4 publique ou d'un nom d'hôte DNS IPv4 public. Votre ordinateur local doit avoir une adresse IPv6 et doit être configuré pour utiliser IPv6. Vous pouvez obtenir l'adresse IPv6 de votre instance à partir de la console Amazon EC2. Consultez la colonne Adresses IPv6 du volet Instances. Vous pouvez également trouver l'adresse IPv6 dans la section d'informations sur l'instance. Lorsque vous sélectionnez l'instance dans le volet Instances de la console Amazon EC2, les informations relatives à cette instance apparaissent dans la partie inférieure de la page. Dans l'onglet Détails, recherchez l'Adresse IPv6.

Si vous préférez, vous pouvez utiliser les commandes [describe-instances](#) (AWS CLI) ou [Get-EC2Instance](#) (AWS Tools for Windows PowerShell). Pour plus d'informations sur IPv6, consultez [Adresses IPv6](#).

- Obtenez le nom d'utilisateur de votre instance.

Vous pouvez vous connecter à votre instance en utilisant le nom d'utilisateur de votre compte utilisateur ou le nom d'utilisateur par défaut de l'AMI que vous avez utilisée pour lancer votre instance.

- Obtenez le nom d'utilisateur de votre compte utilisateur.

Pour plus d'informations sur la création d'un compte utilisateur, consultez [Gérez les utilisateurs du système sur votre instance Linux](#).

- Obtenir le nom d'utilisateur par défaut pour l'AMI que vous avez utilisée pour lancer votre instance :

AMI utilisée pour lancer l'instance	Nom d'utilisateur par défaut
AL2023	ec2-user
Amazon Linux 2	
Amazon Linux	
CentOS	centos ou ec2-user

AMI utilisée pour lancer l'instance	Nom d'utilisateur par défaut
Debian	admin
Fedora	fedora ou ec2-user
RHEL	ec2-user ou root
SUSE	ec2-user ou root
Ubuntu	ubuntu
Oracle	ec2-user
Bitnami	bitnami
Rocky Linux	rocky
Autre	Vérifiez auprès du fournisseur de l'AMI

Localisation de la clé privée et définition des autorisations

Vous devez connaître l'emplacement de votre fichier de clé privée pour vous connecter à votre instance. Pour les connexions SSH, vous devez définir les autorisations afin que vous soyez le seul à pouvoir lire le fichier.

Pour plus d'informations sur le fonctionnement des paires de clés lors de l'utilisation d'Amazon EC2, consultez [Paires de clés Amazon EC2 et instances Amazon EC2](#).

- Localiser la clé privée

Vous aurez besoin du chemin d'accès qualifié complet à l'emplacement sur votre ordinateur du fichier `.pem` pour la paire de clés que vous avez spécifiée lorsque vous avez lancé l'instance. Pour plus d'informations, consultez [the section called "Identifier la clé publique spécifiée au lancement"](#).

Si vous ne trouvez pas votre fichier de clé privée, consultez

[Si vous perdez la clé privée pour une instance basée sur des volumes EBS, vous pouvez à nouveau accéder à votre instance. Vous devez arrêter l'instance, détacher son volume racine et l'attacher à une autre instance en tant que volume de données, modifier le fichier](#)

[authorized_keys](#) avec une nouvelle clé publique, replacer le volume dans l'instance d'origine et redémarrer l'instance. Pour plus d'informations sur le lancement et l'arrêt des instances, ainsi que sur la connexion aux instances, consultez [Cycle de vie d'une instance](#).

Cette procédure est prise en charge uniquement pour des instances avec des volumes racine EBS. Si l'appareil racine est un volume de stockage d'instance, vous ne pouvez pas utiliser cette procédure pour rétablir l'accès à votre instance ; vous devez disposer de la clé privée pour vous connecter à l'instance. Pour déterminer le type d'appareil racine de votre instance, ouvrez la console Amazon EC2, choisissez Instances, sélectionnez l'instance, choisissez l'onglet Stockage, et dans la section Détails de l'appareil racine, vérifiez la valeur du Type d'appareil racine.

La valeur est EBS ou INSTANCE-STORE.

En plus des étapes suivantes, il existe d'autres façons de vous connecter à votre instance Linux en cas de perte de votre clé privée. Pour de plus amples informations, veuillez consulter [Comment puis-je me connecter à mon instance Amazon EC2 si j'ai perdu ma paire de clés SSH après son lancement initial ?](#)

Étapes de connexion à une instance basée sur des volumes EBS avec une paire de clés différente

- [Étape 1 : Créer une nouvelle paire de clés](#)
- [Étape 2 : Obtenir des informations sur l'instance d'origine et son volume racine](#)
- [Étape 3 : Arrêter l'instance d'origine](#)
- [Étape 4 : Lancer une instance temporaire](#)
- [Étape 5 : Détacher le volume racine de l'instance d'origine et l'attacher à l'instance temporaire](#)
- [Étape 6 : Ajouter la nouvelle clé publique `authorized_keys` sur le volume d'origine monté sur l'instance temporaire](#)
- [Étape 7 : Démontez et détachez le volume d'origine de l'instance temporaire, puis le reconnectez à l'instance d'origine](#)
- [Étape 8 : Se connecter à l'instance d'origine à l'aide de la nouvelle paire de clés](#)
- [Étape 9 : nettoyer](#)

Étape 1 : Créer une nouvelle paire de clés

Créer une nouvelle paire de clés à l'aide de la console Amazon EC2 ou d'un outil tiers. Si vous souhaitez nommer votre nouvelle paire de clés exactement comme la clé privée perdue, vous devez commencer par supprimer la paire de clés existante. Pour de plus amples informations sur la création d'une paire de clés, veuillez consulter [Créer une paire de clés à l'aide d'Amazon EC2](#) ou [Créer une paire de clés à l'aide d'un outil tiers et importer la clé publique dans Amazon EC2](#).

Étape 2 : Obtenir des informations sur l'instance d'origine et son volume racine

Notez les informations suivantes, car vous en aurez besoin pour effectuer cette procédure.

Pour obtenir des informations sur votre instance d'origine

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
 2. Choisissez Instances dans le panneau de navigation, puis sélectionnez l'instance à laquelle vous souhaitez vous connecter. (Cette instance est qualifiée d'instance d'origine.)
 3. Sous l'onglet Details (Détails), notez l'ID d'instance et l'ID d'AMI.
 4. Sous l'onglet Networking (Réseaux), notez la zone de disponibilité.
 5. Sous l'onglet Storage (Stockage), sous Root device name (Nom du périphérique racine), notez le nom du périphérique pour le volume racine (par exemple, /dev/xvda). Ensuite, sous Block devices (Bloquer les périphériques), recherchez le nom du périphérique et notez l'ID de volume (par exemple, vol-0a1234b5678c910de).
-

Étape 3 : Arrêter l'instance d'origine

Choisissez État de l'instance, Arrêter l'instance. Si cette option est désactivée, l'instance est déjà arrêtée ou son périphérique racine est un volume de stockage d'instance.

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instance sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

Étape 4 : Lancer une instance temporaire

New console

Pour lancer une instance temporaire

1. Dans le volet de navigation, choisissez Instances, puis Launch instances (Lancer des instances).
 2. Dans la section Name and tags (Noms et identifications), pour Name (Nom), saisissez Temporary (Temporaire).
 3. Dans Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez la même AMI que celle utilisée pour lancer l'instance d'origine. Si l'AMI n'est pas disponible, vous pouvez créer une AMI à utiliser depuis l'instance arrêtée. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).
 4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance par défaut.
 5. Dans la section Key pair (Paire de clés), pour Key pair name (Nom de la paire de clés), sélectionnez une paire de clés existante ou créez-en une.
 6. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis pour Subnet (Sous-réseau), sélectionnez un sous-réseau dans la même zone de disponibilité que celle de l'instance d'origine.
 7. Dans le panneau Summary (Récapitulatif), choisissez Launch (Lancer).
-

Old console

Sélectionnez Launch instances (Lancer des instances), puis utilisez l'assistant de lancement pour lancer une instance temporaire avec les options suivantes :

- Dans la page Choisir une AMI, sélectionnez la même AMI que celle utilisée pour lancer l'instance d'origine. Si l'AMI n'est pas disponible, vous pouvez créer une AMI à utiliser depuis l'instance arrêtée. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).
 - Sur la page Choisir un type d'instance, conservez le type d'instance par défaut sélectionné par l'assistant.
-

- Dans la page Configurer les détails de l'instance, spécifiez la même zone de disponibilité que l'instance d'origine. Si vous lancez une instance dans un VPC, sélectionnez un sous-réseau dans cette zone de disponibilité.
-
- Sur la page Ajouter des balises, ajoutez la balise Name=Temporary à l'instance pour indiquer qu'il s'agit d'une instance temporaire.
-
- Sur la page Review (Vérification), choisissez Launch (Lancer). Sélectionnez la paire de clés que vous avez créée à l'étape 1, puis sélectionnez Launch instances (Lancer les instances).

Étape 5 : Détacher le volume racine de l'instance d'origine et l'attacher à l'instance temporaire

1. Dans le panneau de navigation, sélectionnez Volumes, puis le volume du périphérique racine pour l'instance d'origine (vous avez noté l'ID de volume au cours d'une étape précédente). Choisissez Actions, Detach Volume (Détacher un volume), puis choisissez Detach (Détacher). Attendez que l'état du volume devienne available. (Vous devrez peut-être sélectionner l'icône Actualiser.)
2. Tandis que le volume est toujours sélectionné, choisissez Actions, puis choisissez Attach volume (Attacher un volume). Sélectionnez l'ID d'instance de l'instance temporaire, notez le nom du périphérique spécifié dans Device name (Nom du périphérique) (par exemple, /dev/sdf), puis sélectionnez Attach volume (Attacher un volume).

Note

Si vous avez lancé votre instance d'origine à partir d'une AWS Marketplace AMI et que votre volume contient des AWS Marketplace codes, vous devez d'abord arrêter l'instance temporaire avant de pouvoir attacher le volume.

Étape 6 : Ajouter la nouvelle clé publique **authorized_keys** sur le volume d'origine monté sur l'instance temporaire

1. Connectez-vous à l'instance temporaire.
 2. À partir de l'instance temporaire, montez le volume que vous avez attaché à l'instance afin de pouvoir accéder au système de fichiers. Par exemple, si le nom du périphérique est /
-

`dev/sdf`, utilisez les commandes suivantes pour monter le volume en tant que `/mnt/tempvol`.

Note

Le nom du périphérique peut apparaître différemment sur votre instance. Par exemple, les périphériques montés en tant que `/dev/sdf` peuvent également s'afficher en tant que `/dev/xvdf` sur l'instance. Certaines versions de Red Hat (ou ses variantes, comme CentOS) peuvent même incrémenter la lettre finale de quatre caractères, et `/dev/sdf` devient `/dev/xvdk`.

- a. Utilisez la commande `lsblk` pour déterminer si le volume est divisé.

```
[ec2-user ~]$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda        202:0    0   8G  0 disk
##xvda1    202:1    0   8G  0 part /
xvdf        202:80    0 101G  0 disk
##xvdf1    202:81    0 101G  0 part
xvdg        202:96    0   30G  0 disk
```

Dans l'exemple précédent, `/dev/xvda` et `/dev/xvdf` sont des volumes partitionnés, mais `/dev/xvdg` ne l'est pas. Si votre volume est partitionné, vous montez la partition (`/dev/xvdf1`) au lieu du périphérique brut (`/dev/xvdf`) au cours des étapes suivantes.

- b. Créez un répertoire temporaire pour monter le volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

- c. Montez le volume (ou la partition) sur le point de montage temporaire, en utilisant le nom du volume ou du périphérique que vous avez identifié plus tôt. La commande requise dépend du système de fichiers de votre système d'exploitation. Notez que le nom du périphérique peut apparaître différemment sur votre instance. Reportez-vous à l'étape 6 de [note](#) pour plus d'informations.

- Amazon Linux, Ubuntu et Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 et RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

Note

Si vous obtenez une erreur indiquant que le système de fichiers est endommagé, exécutez la commande suivante pour utiliser l'utilitaire fsck afin de rechercher les erreurs dans votre système de fichiers et de les résoudre.

```
[ec2-user ~]$ sudo fsck /dev/xvdf1
```

3. À partir de l'instance temporaire, utilisez la commande suivante pour mettre à jour `authorized_keys` sur le volume monté avec la nouvelle clé publique de `authorized_keys` pour l'instance temporaire.

Important

Les exemples suivants utilisent le nom d'utilisateur Amazon Linux `ec2-user`. Vous devrez peut-être modifier le nom d'utilisateur, par exemple, `ubuntu` pour les instances Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/  
authorized_keys
```

Une fois que cette étape est correctement effectuée, vous pouvez passer à l'étape suivante. (Facultatif) Sinon, si vous n'êtes pas autorisé à modifier des fichiers dans `/mnt/tempvol`, vous devez mettre à jour le fichier à l'aide de la commande `sudo`, puis vérifier les autorisations sur le fichier afin de vous assurer que vous êtes en mesure de vous connecter à l'instance d'origine. Pour vérifier les autorisations sur le fichier, utilisez la commande suivante.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

```
total 4
-rw----- 1 222 500 398 Sep 13 22:54 authorized_keys
```

Dans cet exemple, **222** est l'ID d'utilisateur et **500** est l'ID de groupe. Utilisez ensuite la commande `sudo` pour ré-exécuter la commande `cp` ayant échoué.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Exécutez à nouveau la commande suivante pour déterminer si les autorisations ont été modifiées.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Si l'ID d'utilisateur et l'ID de groupe ont été modifiés, utilisez la commande suivante pour les restaurer.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Étape 7 : Démontez et détachez le volume d'origine de l'instance temporaire, puis reconnectez à l'instance d'origine

1. À partir de l'instance temporaire, démontez le volume que vous avez attaché afin de pouvoir l'attacher à nouveau à l'instance d'origine. Par exemple, utilisez la commande suivante pour démonter le volume situé dans `/mnt/tempvol`.

```
[ec2-user ~]$ sudo umount /mnt/tempvol
```

2. Détachez le volume de l'instance temporaire (vous l'avez démonté à l'étape précédente) : dans la console Amazon EC2, choisissez `Volumes` dans le panneau de navigation, sélectionnez le volume du périphérique racine de l'instance d'origine (vous avez noté l'ID de volume à l'étape précédente), sélectionnez `Actions`, `Detach volume` (Détacher un volume), puis `Detach` (Détacher). Attendez que l'état du volume devienne `available`. (Vous devrez peut-être sélectionner l'icône `Actualiser`.)

3. Rattachez le volume à l'instance d'origine : le volume étant toujours sélectionné, choisissez Actions, Attach volume (Attacher un volume). Sélectionnez l'ID d'instance de l'instance

d'origine, précisez le nom de l'appareil que vous avez noté précédemment au cours de l'étape 2 pour l'attachement de l'appareil racine d'origine (/dev/sda1 ou /dev/xvda), puis choisissez Attach volume (Attacher un volume).

 Important

Si vous ne spécifiez pas le même nom de périphérique que pour l'attachement original, vous ne pourrez pas démarrer l'instance d'origine. Amazon EC2 s'attend à ce que le volume du périphérique racine soit sda1 ou /dev/xvda.

Étape 8 : Se connecter à l'instance d'origine à l'aide de la nouvelle paire de clés

Sélectionnez l'instance d'origine, choisissez État de l'instance, Démarrer l'instance. Lorsque l'état de l'instance est `running`, vous pouvez vous y connecter à l'aide du fichier de clé privée de votre nouvelle paire de clés.

 Note

Si le nom de votre paire de clés et du fichier de clé privée correspondant est différent du nom de la paire de clés initiale, veuillez à spécifier le nom du nouveau fichier de clé privée lorsque vous vous connectez à votre instance.

Étape 9 : nettoyer

(Facultatif) Vous pouvez mettre fin à l'instance temporaire si vous n'en avez plus besoin.

Sélectionnez l'instance temporaire, puis Instance State (État de l'instance) et `Terminate instance` (Résilier l'instance).

Si vous vous connectez à votre instance à l'aide de Putty et que vous devez convertir le fichier `.pem` au format `.ppk`, consultez [Convertir votre clé privée avec PuTTYgen](#) dans la rubrique [Connexion à votre instance Linux à partir de Windows à l'aide de PuTTY](#) de cette section.

- Définissez les autorisations de votre clé privée de manière à ce que vous soyez le seul à pouvoir la lire

- Connexion à partir de macOS ou Linux

(Instances Linux) Si vous envisagez d'utiliser un client SSH sur un ordinateur macOS ou Linux pour vous connecter à votre instance Linux, utilisez la commande suivante pour définir les autorisations de votre fichier de clé privée afin que vous soyez le seul à pouvoir le lire.

```
chmod 400 key-pair-name.pem
```

Si vous ne définissez pas ces autorisations, vous ne pouvez pas vous connecter à votre instance à l'aide de cette paire de clés. Pour plus d'informations, consultez [Erreur : fichier de clé privée non protégé](#).

- Connexion à partir de Windows

Ouvrez l'Explorateur de fichiers et cliquez avec le bouton droit sur le fichier .pem. Sélectionnez Propriétés > l'onglet Sécurité et choisissez Avancé. Choisissez Désactiver l'héritage. Supprimez l'accès à tous les utilisateurs à l'exception de l'utilisateur actuel.

(Facultatif) Obtenez l'empreinte digitale de l'instance

Pour vous protéger des man-in-the-middle attaques, vous pouvez vérifier l'authenticité de l'instance à laquelle vous allez vous connecter en vérifiant l'empreinte digitale affichée. La vérification de l'empreinte digitale est utile si vous avez lancé votre instance à partir d'une AMI publique fournie par un tiers.

Présentation de la tâche

Tout d'abord, récupérez l'empreinte digitale de l'instance. Ensuite, lorsque vous vous connectez à l'instance et que vous êtes invité à vérifier l'empreinte digitale, comparez l'empreinte que vous avez obtenue au cours de cette procédure avec l'empreinte digitale affichée. Si les empreintes digitales ne correspondent pas, quelqu'un est peut-être en train de tenter une man-in-the-middle attaque. Si elles correspondent, vous pouvez vous connecter à votre instance en toute confiance.

Conditions préalables pour obtenir l'empreinte digitale de l'instance

- L'instance ne doit pas être dans l'état pending. L'empreinte digitale n'est disponible qu'une fois le premier démarrage de l'instance terminé.
- Vous devez être le propriétaire de l'instance pour obtenir la sortie de la console.

- Il existe différentes manières d'obtenir l'empreinte digitale de l'instance. Si vous souhaitez utiliser le AWS CLI, il doit être installé sur votre ordinateur local. Pour plus d'informations sur l'installation du AWS CLI, reportez-vous à la section [Installation du AWS Command Line Interface](#) dans le guide de AWS Command Line Interface l'utilisateur.

Pour obtenir l'empreinte digitale de l'instance

À l'étape 1, vous obtenez la sortie de la console, qui inclut l'empreinte digitale de l'instance. À l'étape 2, vous trouverez l'empreinte de l'instance dans la sortie de la console.

1. Obtenez le résultat de la console à l'aide de l'une des méthodes suivantes.

Console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le navigateur de gauche, sélectionnez Instances.
3. Sélectionnez votre instance, puis choisissez Actions, Surveiller et dépanner, puis Obtenir le journal du système.

AWS CLI

Sur votre ordinateur local (et non sur l'instance à laquelle vous vous connectez), utilisez la commande [get-console-output](#) ().AWS CLI Si la sortie est volumineuse, [vous pouvez la diriger vers un fichier texte](#) où elle sera peut-être plus facile à lire. Notez que vous devez spécifier un Région AWS lorsque vous utilisez le AWS CLI, soit explicitement, soit en définissant une région par défaut. Pour plus d'informations sur la définition ou la spécification d'une région, consultez [Principes de base de la configuration](#) dans le Guide de l'utilisateur AWS Command Line Interface .

```
aws ec2 get-console-output --instance-id instance_id --query Output --output text > temp.txt
```

2. Dans la sortie de console, recherchez l'empreinte digitale de l'instance (hôte), qui se trouve sous BEGIN SSH HOST KEY FINGERPRINTS. Il peut y avoir plusieurs exemples d'empreintes digitales. Lorsque vous vous connectez à votre instance, celle-ci n'affiche qu'une seule des empreintes digitales.

La sortie exacte peut varier selon le système d'exploitation, la version AMI et si AWS a créé la clé. Voici un exemple de sortie.

```
ec2:#####  
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----  
ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)  
ec2: 256 SHA256:kpEa+rW/Uq3zxaYZN8KT501iBtJ0IdHG52dFi66EEfQ no comment (ED25519)  
ec2: 2048 SHA256:L816pepcA7iqW/jBecQjVZC1UrKY+o2cHLI0iHerbVc no comment (RSA)  
ec2: -----END SSH HOST KEY FINGERPRINTS-----  
ec2: #####
```

Note

Vous ferez référence à cette empreinte lorsque vous vous connecterez à l'instance.

Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH

Vous pouvez utiliser Secure Shell (SSH) pour vous connecter à votre instance Linux depuis une machine locale qui exécute un système d'exploitation Linux ou macOS, ou vous pouvez utiliser un outil de connexion indépendant de la plate-forme, tel qu'EC2 Instance Connect ou AWS Systems Manager Session Manager. Pour plus d'informations sur les outils indépendants de la plateforme, veuillez consulter la rubrique [Connectez-vous à votre instance Linux](#).

Cette page explique comment se connecter à votre instance via un client SSH. Pour vous connecter à votre instance Linux à partir de Windows, veuillez consulter la rubrique [Connexion à partir de Windows](#).

Note

Si vous recevez un message d'erreur lorsque vous tentez de vous connecter à votre instance, assurez-vous que celle-ci répond à toutes les [Conditions préalables pour la connexion SSH](#). Si elle répond à toutes les conditions préalables et que vous ne parvenez toujours pas à vous connecter à votre instance Linux, veuillez consulter la rubrique [Résoudre les problèmes de connexion à votre instance Linux](#).

Table des matières

- [Conditions préalables pour la connexion SSH](#)
- [Connexion à votre instance Linux à l'aide d'un client SSH](#)
- [Transférer des fichiers vers des instances Linux à l'aide d'un client SCP](#)

Conditions préalables pour la connexion SSH

Avant de vous connecter à votre instance Linux, remplissez les prérequis suivants.

Vérifier l'état de votre instance

Une fois l'instance lancée, il peut falloir quelques minutes pour qu'elle soit prête pour que vous puissiez vous y connecter. Vérifiez que votre instance a réussi les contrôles de statut. Vous pouvez afficher ces informations dans la colonne Status check (Vérification de statut) de la page instances.

Obtenir le nom DNS public et le nom d'utilisateur pour se connecter à votre instance

Pour rechercher le nom DNS public ou l'adresse IP de votre instance et le nom d'utilisateur que vous devez utiliser pour vous connecter à cette dernière, consultez [Obtenez des informations sur votre instance](#).

Rechercher la clé privée et définir les autorisations

Pour localiser la clé privée requise pour se connecter à votre instance et pour définir les autorisations de clé, consultez [Localisation de la clé privée et définition des autorisations](#).

Installez un client SSH sur votre ordinateur local, si besoin.

Un client SSH peut être installé par défaut sur votre ordinateur local. Vous pouvez vérifier cela en tapant ssh sur la ligne de commande. Si votre ordinateur ne reconnaît pas la commande, vous pouvez installer un client SSH pour vous connecter au nœud maître.

- Versions récentes de Windows Server 2019 et Windows 10 – OpenSSH est inclus en tant que composant installable. Pour plus d'informations, consultez [OpenSSH dans Windows](#).
- Versions antérieures de Windows – Téléchargez et installez OpenSSH. Pour plus d'informations, consultez [Win32-OpenSSH](#).
- Linux et macOS X – Téléchargez et installez OpenSSH. Pour plus d'informations, consultez <https://www.openssh.com>.

Connexion à votre instance Linux à l'aide d'un client SSH

Utilisez la procédure suivante pour vous connecter à votre instance Linux à l'aide d'un client SSH. Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [Résoudre les problèmes de connexion à votre instance Linux](#).

Se connecter à votre instance à l'aide de SSH

1. Utilisez la commande `ssh` dans une fenêtre de terminal pour vous connecter à l'instance. Vous spécifiez le chemin et le nom de fichier de la clé privée (.pem), le nom d'utilisateur de votre AMI et le nom DNS public ou l'adresse IPv6 de votre instance. Pour savoir comment trouver la clé privée, le nom d'utilisateur d'une instance et le nom DNS ou l'adresse IPv6 d'une instance, consultez [Localisation de la clé privée et définition des autorisations](#) et [Obtenez des informations sur votre instance](#). Pour vous connecter à votre instance, utilisez l'une des commandes suivantes.

- (DNS public) Pour vous connecter à l'aide du nom DNS public de votre instance, entrez la commande suivante.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Sinon, si votre instance possède une adresse IPv6, pour vous connecter en utilisant l'adresse IPv6 de votre instance, entrez la commande suivante.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

Vous verrez une réponse telle que celle ci-après:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'  
can't be established.  
ECDSA key fingerprint is 14UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.  
Are you sure you want to continue connecting (yes/no)?
```

2. (Facultatif) Vérifiez que l'empreinte de l'alerte de sécurité correspond à l'empreinte que vous avez précédemment obtenue dans [\(Facultatif\) Obtenez l'empreinte digitale de l'instance](#). Si ces empreintes ne correspondent pas, il se peut que quelqu'un tente une man-in-the-middle attaque. Si elles correspondent, passez à l'étape suivante.
3. Saisissez **yes**.

Vous verrez une réponse telle que celle ci-après:

Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to the list of known hosts.

Transférer des fichiers vers des instances Linux à l'aide d'un client SCP

Le transfert de fichiers entre votre ordinateur local et une instance Linux peut se faire en le protocole de copie sécurisée (SCP). Cette section décrit comment transférer des fichiers avec SCP. La procédure est similaire à celle de la connexion à une instance avec SSH.

Prérequis

- Vérifiez les prérequis généraux pour le transfert de fichiers à votre instance.

Avant de transférer des fichiers entre votre ordinateur local et votre instance, effectuez les actions suivantes pour vous assurer que vous disposez de toutes les informations dont vous avez besoin.

- [Obtenez des informations sur votre instance](#)
- [Localisation de la clé privée et définition des autorisations](#)
- [\(Facultatif\) Obtenez l'empreinte digitale de l'instance](#)
- Installez un client SCP

La plupart des ordinateurs Linux, Unix et Apple comporte un client SCP par défaut. Si ce n'est pas le cas pour le vôtre, le projet OpenSSH offre une implémentation gratuite de l'ensemble de la suite d'outils SSH, notamment un client SCP. Pour plus d'informations, consultez <https://www.openssh.com>.

La procédure suivante vous aide à utiliser SCP pour transférer un fichier en utilisant le nom DNS public de l'instance ou l'adresse IPv6 si votre instance en possède un.

Pour utiliser SCP pour transférer des fichiers entre votre ordinateur et votre instance

1. Déterminez l'emplacement du fichier source sur votre ordinateur et le chemin d'accès de destination sur l'instance. Dans les exemples suivants, le nom du fichier de clé privée est `key-pair-name.pem`, le fichier à transférer est `my-file.txt`, le nom d'utilisateur de l'instance est `ec2-user`, le nom DNS public de l'instance est `instance-public-dns-name` et l'adresse IPv6 de l'instance est `instance-IPv6-address`.

- (DNS public) Pour transférer un fichier vers la destination de l'instance, entrez la commande suivante à partir de votre ordinateur.

```
scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
```

- (IPv6) Pour transférer un fichier vers la destination de l'instance si l'instance possède une adresse IPv6, entrez la commande suivante à partir de votre ordinateur. L'adresse IPv6 doit être placée entre crochets ([]), lesquels doivent être précédés d'un caractère d'échappement (\).

```
scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@[instance-IPv6-address]:path/
```

2. Si vous ne vous êtes pas encore connecté à l'instance à l'aide de SSH, la réponse suivante devrait s'afficher :

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

(Facultatif) Vous pouvez vérifier si l'empreinte digitale de l'alerte de sécurité correspond à l'empreinte digitale de l'instance. Pour plus d'informations, consultez [\(Facultatif\) Obtenez l'empreinte digitale de l'instance](#).

Saisissez **yes**.

3. Si le transfert réussit, la réponse est semblable à la suivante :

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                               100%  480    24.4KB/s   00:00
```

4. Pour transférer un fichier dans l'autre direction (de votre instance Amazon EC2 à votre ordinateur), inversez l'ordre des paramètres de l'hôte. Par exemple, vous pouvez transférer `my-file.txt` de votre instance EC2 vers une destination sur votre ordinateur local en tant que `my-file2.txt`, comme illustré dans les exemples suivants.
 - (DNS public) Pour transférer un fichier vers une destination sur votre ordinateur, entrez la commande suivante à partir de votre ordinateur.

```
scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-file.txt path/my-file2.txt
```

- (IPv6) Pour transférer un fichier vers une destination sur votre ordinateur si l'instance possède une adresse IPv6, entrez la commande suivante à partir de votre ordinateur. L'adresse IPv6 doit être placée entre crochets ([]), lesquels doivent être précédés d'un caractère d'échappement (\).

```
scp -i /path/key-pair-name.pem ec2-user@[instance-IPv6-address]:path/my-file.txt path/my-file2.txt
```

Connexion à votre instance Linux à partir de Windows

Vous pouvez utiliser les méthodes suivantes pour vous connecter à votre instance Linux à partir d'une machine locale dotée d'un système d'exploitation Windows.

Connexion à votre instance Linux à partir de Windows à l'aide d'OpenSSH

Les procédures suivantes vous montrent comment vous connecter à votre instance Linux à partir de Windows en utilisant OpenSSH, un outil de connectivité open source pour la connexion à distance à l'aide du protocole SSH. OpenSSH est pris en charge sur les systèmes d'exploitation Windows Server 2019 et versions ultérieures.

Table des matières

- [Prérequis](#)
- [Installez OpenSSH pour Windows à l'aide de PowerShell](#)
- [Se connecter à votre instance Linux à partir de Windows à l'aide d'OpenSSH](#)
- [Désinstallez OpenSSH de Windows à l'aide de PowerShell](#)

Prérequis

Avant de vous connecter à votre instance Linux depuis Windows à l'aide d'OpenSSH, vérifiez les conditions préalables suivantes.

Vérifiez que l'instance est prête.

Une fois l'instance lancée, il peut falloir quelques minutes pour qu'elle soit prête pour que vous puissiez vous y connecter. Vérifiez que votre instance a réussi les contrôles de statut. Vous pouvez afficher ces informations dans la colonne Status check (Vérification de statut) de la page instances.

Vérifiez les prérequis généraux pour la connexion à votre instance.

Pour rechercher le nom DNS public ou l'adresse IP de votre instance et le nom d'utilisateur que vous devez utiliser pour vous connecter à cette dernière, veuillez consulter la rubrique [Obtenez des informations sur votre instance](#).

Vérifiez votre version Windows

Pour vous connecter à votre instance Linux depuis Windows à l'aide d'OpenSSH, la version Windows doit être Windows Server 2019 et versions ultérieures.

Vérifiez les PowerShell prérequis

Pour installer OpenSSH sur votre système d'exploitation Windows à PowerShell l'aide de la version 5.1 ou ultérieure, et votre compte doit être membre du groupe d'administrateurs intégré. PowerShell Exécutez PowerShell à \$PSVersionTable.PSVersion partir de pour vérifier votre PowerShell version.

Pour vérifier si vous êtes membre du groupe d'administrateurs intégré, exécutez la PowerShell commande suivante :

```
(New-Object Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Si vous êtes membre du groupe d'administrateurs intégré, le résultat est True.

Installez OpenSSH pour Windows à l'aide de PowerShell

Pour installer OpenSSH pour Windows à l'aide de PowerShell, exécutez la commande suivante :

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Sortie attendue :

```
Path      :  
Online    : True  
RestartNeeded : False
```

Se connecter à votre instance Linux à partir de Windows à l'aide d'OpenSSH

Après avoir installé OpenSSH, utilisez la procédure suivante pour vous connecter à votre instance Linux à partir de Windows à l'aide d'OpenSSH. Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [Résoudre les problèmes de connexion à votre instance Linux](#).

Pour vous connecter à votre instance à l'aide d'OpenSSH

1. Dans PowerShell ou dans l'invite de commande, utilisez la ssh commande pour vous connecter à l'instance. Vous spécifiez le chemin et le nom de fichier de la clé privée (.pem), le nom d'utilisateur de votre instance et le nom DNS public ou l'adresse IPv6 de votre instance. Pour savoir comment trouver la clé privée, le nom d'utilisateur d'une instance et le nom DNS ou l'adresse IPv6 d'une instance, veuillez consulter les rubriques [Localisation de la clé privée et définition des autorisations](#) et [Obtenez des informations sur votre instance](#). Pour vous connecter à votre instance, utilisez l'une des commandes suivantes.

- (DNS public) Pour vous connecter à l'aide du nom DNS public de votre instance, entrez la commande suivante.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Sinon, si votre instance possède une adresse IPv6, pour vous connecter en utilisant l'adresse IPv6 de votre instance, entrez la commande suivante.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

Vous verrez une réponse telle que celle ci-après:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'  
can't be established.  
ECDSA key fingerprint is 14UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.  
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

2. (Facultatif) Vérifiez que l'empreinte de l'alerte de sécurité correspond à l'empreinte que vous avez précédemment obtenue dans [\(Facultatif\) Obtenez l'empreinte digitale de l'instance](#). Si ces

empreintes ne correspondent pas, il se peut que quelqu'un tente une man-in-the-middle attaque. Si elles correspondent, passez à l'étape suivante.

3. Saisissez **yes**.

Vous verrez une réponse telle que celle ci-après:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to the list of known hosts.
```

Désinstallez OpenSSH de Windows à l'aide de PowerShell

Pour désinstaller OpenSSH de Windows à l'aide de PowerShell, exécutez la commande suivante :

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Sortie attendue :

```
Path          :
Online        : True
RestartNeeded : True
```

Connexion à votre instance Linux à partir de Windows à l'aide de PuTTY

Si vous utilisez Windows Server 2019 ou une version ultérieure, nous vous recommandons d'utiliser OpenSSH, un outil de connectivité open source pour la connexion à distance via le protocole SSH. Pour la procédure à suivre pour vous connecter à une instance Linux depuis Windows à l'aide d'OpenSSH, veuillez consulter [Connexion à votre instance Linux à partir de Windows à l'aide d'OpenSSH](#).

Les instructions suivantes expliquent comment vous connecter à votre instance à l'aide de PuTTY, un client SSH gratuit pour Windows. Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [Résoudre les problèmes de connexion à votre instance Linux](#).

Table des matières

- [Prérequis](#)
 - [Convertir votre clé privée avec PuTTYgen](#)

- [Connectez-vous à votre instance Linux](#)
- [Transférer des fichiers vers votre instance Linux à l'aide du client Secure Copy PuTTY](#)
- [Transférer des fichiers vers votre instance Linux à l'aide de WinSCP](#)

Prérequis

Avant de vous connecter à votre instance Linux à l'aide de PuTTY, remplissez les prérequis suivants.

Vérifiez que l'instance est prête.

Une fois l'instance lancée, il peut falloir quelques minutes pour qu'elle soit prête pour que vous puissiez vous y connecter. Vérifiez que votre instance a réussi les contrôles de statut. Vous pouvez afficher ces informations dans la colonne Status check (Vérification de statut) de la page instances.

Vérifiez les prérequis généraux pour la connexion à votre instance.

Pour rechercher le nom DNS public ou l'adresse IP de votre instance et le nom d'utilisateur que vous devez utiliser pour vous connecter à cette dernière, veuillez consulter la rubrique [Obtenez des informations sur votre instance](#).

Installez PuTTY sur votre ordinateur local.

Téléchargez et installez PuTTY à partir de la [page de téléchargement PuTTY](#). Si une version antérieure de PuTTY est installée, nous vous recommandons de télécharger la dernière version. Assurez-vous d'installer toute la suite.

Convertir votre clé .pem privée au format .ppk avec PuTTYgen

Pour la paire de clés que vous avez spécifiée lors du lancement de l'instance, si vous avez choisi de créer la clé privée au format .pem, vous devez la convertir en un fichier .ppk pour l'utiliser avec PuTTY. Localisez le fichier .pem privé, puis suivez les étapes de la section suivante.

Convertir votre clé privée avec PuTTYgen

PuTTY ne prend pas en charge de manière native le format PEM pour les clés SSH. PuTTY fournit un outil nommé PuTTYgen, qui convertit les clés PEM au format PPK requis pour PuTTY. Vous devez convertir votre clé privée (fichier .pem) dans ce format (fichier .ppk) comme suit pour vous connecter à votre instance avec PuTTY.

Pour convertir votre clé .pem privée au format .ppk.

1. Depuis le menu Start (Démarrer), choisissez All Programs (Tous les programmes), PuTTY, PuTTYgen.
2. Sous Type of key to generate (Type de clé à générer), sélectionnez RSA. Si votre version de PuTTYgen n'inclut pas cette option, choisissez SSH-2 RSA.



3. Choisissez Load (Charger). Par défaut, PuTTYgen affiche uniquement les fichiers ayant l'extension .ppk. Pour trouver votre fichier .pem, choisissez l'option permettant d'afficher tous les types de fichiers.



4. Sélectionnez votre fichier .pem pour la paire de clés que vous avez spécifiée lorsque vous avez lancé votre instance, puis choisissez Ouvrir. PuTTYgen affiche une notification indiquant que le fichier .pem a été importé avec succès. Choisissez OK.
5. Pour enregistrer la clé privée dans un format qui peut être utilisé avec PuTTY, choisissez Enregistrer clé privée. PuTTYgen affiche un avertissement sur l'enregistrement de la clé sans une phrase passe. Choisissez Oui.

Note

La phrase secrète d'une clé privée constitue une couche supplémentaire de protection. Même si votre clé privée est découverte, elle ne peut pas être utilisée sans la phrase secrète. Le désavantage d'une phrase secrète est qu'elle rend l'automatisation plus difficile, car l'intervention humaine est nécessaire pour se connecter à une instance, ou copier des fichiers vers une instance.

6. Spécifiez le même nom pour la clé que celui que vous avez utilisé pour la paire de clés (par exemple, key-pair-name) et choisissez Enregistrer. PuTTY ajoute automatiquement l'extension de fichier .ppk.

Votre clé privée est désormais dans bon format pour être utilisée avec PuTTY. Vous pouvez désormais vous connecter à votre instance en utilisant le client SSH de PuTTY.

Connectez-vous à votre instance Linux

Utilisez la procédure suivante pour vous connecter à votre instance Linux à l'aide de PuTTY. Vous aurez besoin du fichier .ppk que vous avez créé pour votre clé privée. Pour plus d'informations, consultez [Convertir votre clé privée avec PuTTYgen](#) dans la section précédente. Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [Résoudre les problèmes de connexion à votre instance Linux](#).

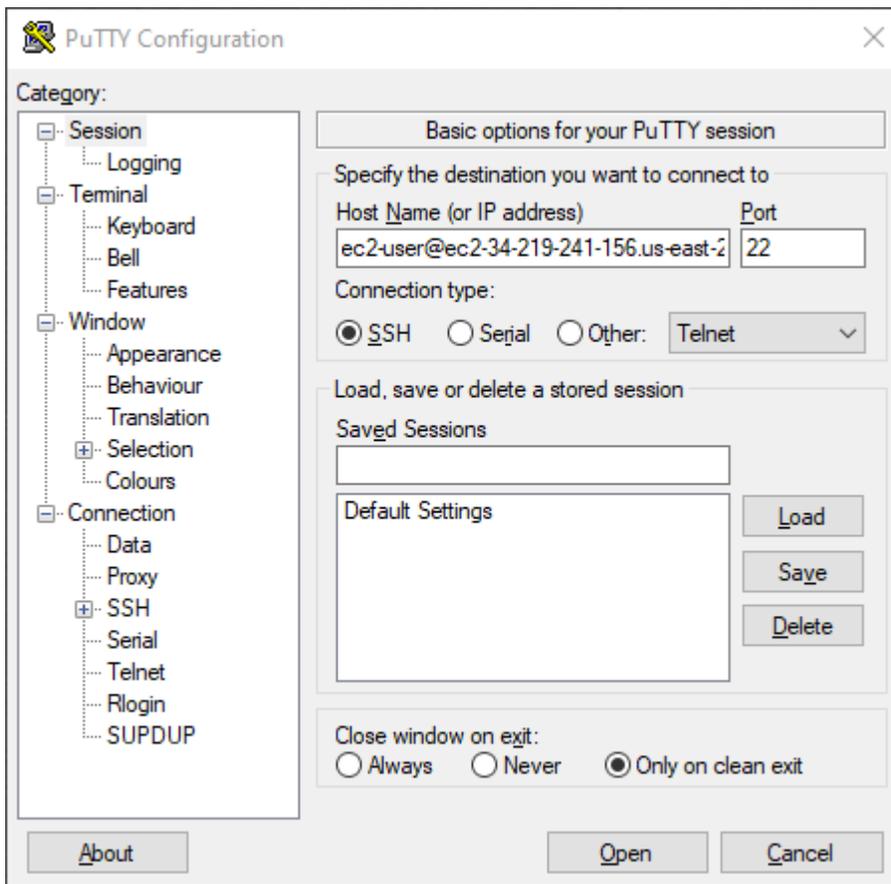
Dernière version testée de PuTTY : .78

Pour vous connecter à votre instance à l'aide de PuTTY

1. Démarrez PuTTY (dans le menu Démarrer, recherchez PuTTY, puis choisissez Ouvrir).
2. Dans le volet Catégorie, Choisissez Session et complétez les champs suivants :
 - a. Dans la zone Host Name (Nom d'hôte), effectuez l'une des opérations suivantes :
 - (DNS public) Pour vous connecter à l'aide du nom DNS public de votre instance, saisissez *instance-user-name@instance-public-dns-name*.
 - (IPv6) Sinon, si votre instance possède une adresse IPv6, pour vous connecter en utilisant l'adresse IPv6 de votre instance, saisissez *instance-user-name@instance-IPv6-address*.

Pour plus d'informations sur la façon d'obtenir le nom d'utilisateur de votre instance, ainsi que le nom DNS public ou l'adresse IPv6 de votre instance, veuillez consulter la rubrique [Obtenez des informations sur votre instance](#).

- b. Vérifiez que Port a pour valeur 22.
- c. Sous Type de connexion, sélectionnez SSH.



3. (Facultatif) Vous pouvez configurer PuTTY pour envoyer automatiquement des données « keepalive » à intervalles réguliers afin de garder votre session active. Cela est particulièrement utile et vous évite de vous déconnecter de votre instance en raison de l'inactivité de la session. Dans le volet Catégorie, choisissez Connexion, puis entrez l'intervalle requis dans le champ Secondes écoulées entre les paquets keepalive. Par exemple, si votre session se déconnecte après 10 minutes d'inactivité, entrez 180 pour configurer PuTTY pour envoyer des données keepalive toutes les 3 minutes.
4. Dans le volet Catégorie, développez Connexion, SSH, puis choisissez Auth. Choisissez Informations d'identification.
5. À côté de Fichier de clé privée pour l'authentification, choisissez Parcourir. Dans la boîte de dialogue Sélectionner le fichier de clé privée, sélectionnez le fichier .ppk que vous avez généré pour votre paire de clés. Vous pouvez soit double-cliquer sur le fichier, soit choisir Ouvrir dans la boîte de dialogue Sélectionner un fichier de clé privée.
6. (Facultatif) Si vous comptez vous reconnecter à cette instance après cette session, vous pouvez enregistrer les informations correspondantes pour les utiliser à l'avenir. Dans le volet Catégorie,

choisissez Session. Saisissez un nom pour la session dans Sessions enregistrées, puis choisissez Enregistrer.

7. Pour vous connecter à l'instance, choisissez Ouvrir.
8. S'il s'agit de votre première connexion à cette instance, PuTTY affiche une boîte de dialogue d'alerte de sécurité qui vous demande si vous faites confiance à l'hôte auquel vous vous connectez.
 - a. (Facultatif) Vérifiez que l'empreinte dans la boîte de dialogue d'alerte de sécurité correspond à l'empreinte que vous avez obtenue précédemment dans [\(Facultatif\) Obtenez l'empreinte digitale de l'instance](#). Si ces empreintes ne correspondent pas, quelqu'un essaie peut-être d'effectuer une attaque MITM. Si elles correspondent, passez à l'étape suivante.
 - b. Choisissez Accepter. Une fenêtre s'ouvre et vous êtes connecté à votre instance.

 Note

Si vous avez spécifié une phrase de passe lorsque vous avez converti votre clé privée au format PuTTY, vous devez fournir cette phrase de passe au moment de la connexion à l'instance.

Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [Résoudre les problèmes de connexion à votre instance Linux](#).

Transférer des fichiers vers votre instance Linux à l'aide du client Secure Copy PuTTY

Le client Secure Copy PuTTY (PSCP) est un outil de ligne de commande que vous pouvez utiliser pour transférer les fichiers entre votre ordinateur Windows et votre instance Linux. Si vous préférez une interface utilisateur graphique (GUI), vous pouvez utiliser un outil GUI open source nommé WinSCP. Pour plus d'informations, consultez [Transférer des fichiers vers votre instance Linux à l'aide de WinSCP](#).

Pour utiliser PSCP, vous aurez besoin de la clé privée que vous avez générée dans [Convertir votre clé privée avec PuTTYgen](#). Vous avez également besoin du nom DNS public de votre instance Linux, ou de l'adresse IPv6 si votre instance en a une.

Dans l'exemple suivant, le fichier `Sample_file.txt` est transféré depuis le lecteur C:\ d'un ordinateur Windows vers le répertoire de base `instance-user-name` d'une instance Amazon Linux. Pour transférer un fichier, utilisez l'une des commandes suivantes.

- (DNS public) Pour transférer un fichier à l'aide du nom DNS public de votre instance, entrez la commande suivante.

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@instance-public-dns-name:/home/instance-user-name/Sample_file.txt
```

- (IPv6) Sinon, si votre instance possède une adresse IPv6, pour vous connecter en utilisant l'adresse IPv6 de votre instance, entrez la commande suivante. L'adresse IPv6 doit être entre crochets ([]).

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@[instance-IPv6-address]:/home/instance-user-name/Sample_file.txt
```

Transférer des fichiers vers votre instance Linux à l'aide de WinSCP

WinSCP est un gestionnaire de fichiers basé sur l'interface utilisateur graphique pour Windows qui vous permet de charger et de transférer des fichiers vers un ordinateur distant à l'aide des protocoles SFTP, SCP, FTP, et FTPS. WinSCP vous donne la possibilité de glisser et déposer les fichiers de votre ordinateur Windows vers votre instance Linux ou de synchroniser des structures entières de répertoires entre les deux systèmes.

Prérequis

- Vous devez disposer de la clé privée que vous avez générée dans [Convertir votre clé privée avec PuTTYgen](#).
- Vous avez également besoin du nom DNS public de votre instance Linux.
- Le package scp doit être installé sur votre instance Linux. Pour certains systèmes d'exploitation, vous installez le package openssh-clients. Pour d'autres, tels que l'AMI optimisé pour Amazon ECS, vous installez le scp package. Consultez la documentation de votre distribution Linux.

Pour vous connecter à votre instance à l'aide de WinSCP

1. Téléchargez et installez WinSCP à partir de <http://winscp.net/eng/download.php>. Pour la plupart des utilisateurs, les options d'installation par défaut sont correctes.
2. Démarrez WinSCP.
3. Dans l'écran Connexion WinSCP pour Nom d'hôte, entrez l'une des options suivantes :

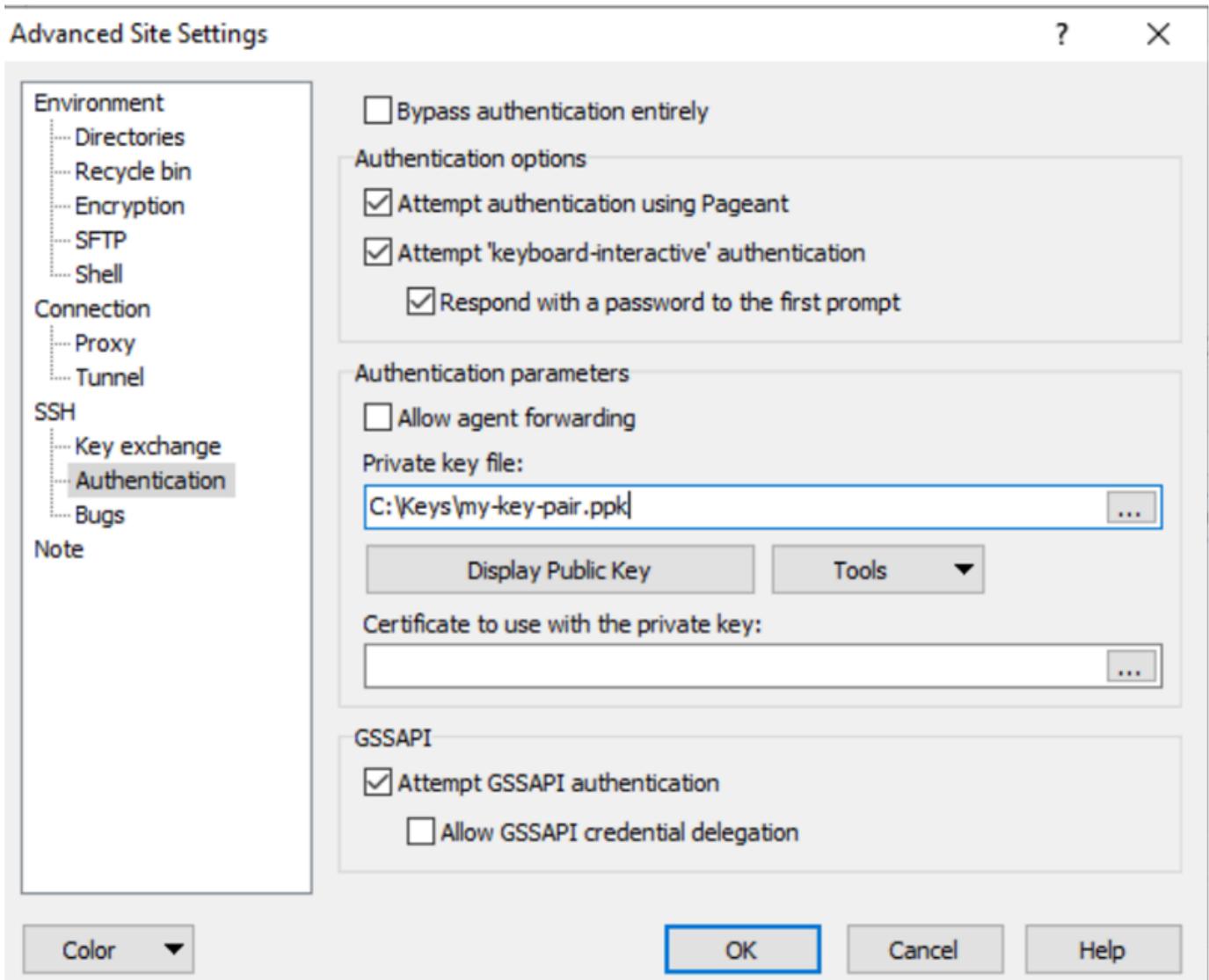
- (Adresse DNS publique ou IPv4) Pour vous connecter à l'aide du nom DNS public ou de l'adresse IPv4 publique de votre instance, entrez le nom DNS public ou l'adresse IPv4 publique de votre instance.
 - (IPv6) Sinon, si votre instance possède une adresse IPv6, pour vous connecter en utilisant l'adresse IPv6 de votre instance, entrez l'adresse IPv6 de votre instance.
4. Pour Nom d'utilisateur, saisissez le nom utilisateur par défaut pour votre AMI.
- Pour AL2023, Amazon Linux 2 ou l'AMI Amazon Linux, le nom d'utilisateur est `ec2-user`.
 - Pour une AMI CentOS, le nom d'utilisateur est `centos` ou `ec2-user`.
 - Pour une AMI Debian, le nom d'utilisateur est `admin`.
 - Pour une AMI Fedora, le nom d'utilisateur est `fedora` ou `ec2-user`.
 - Pour une AMI RHEL, le nom d'utilisateur est `root` ou `ec2-user`.
 - Pour une AMI SUSE, le nom d'utilisateur est `ec2-user` ou `root`.
 - Pour une AMI Ubuntu, le nom utilisateur est `ubuntu`.
 - Pour une AMI Oracle, le nom d'utilisateur est `ec2-user`.
 - Pour une AMI Bitnami, le nom d'utilisateur est `bitnami`.

 Note

Pour trouver le nom d'utilisateur par défaut pour les autres distributions Linux, contactez le fournisseur d'AMI.

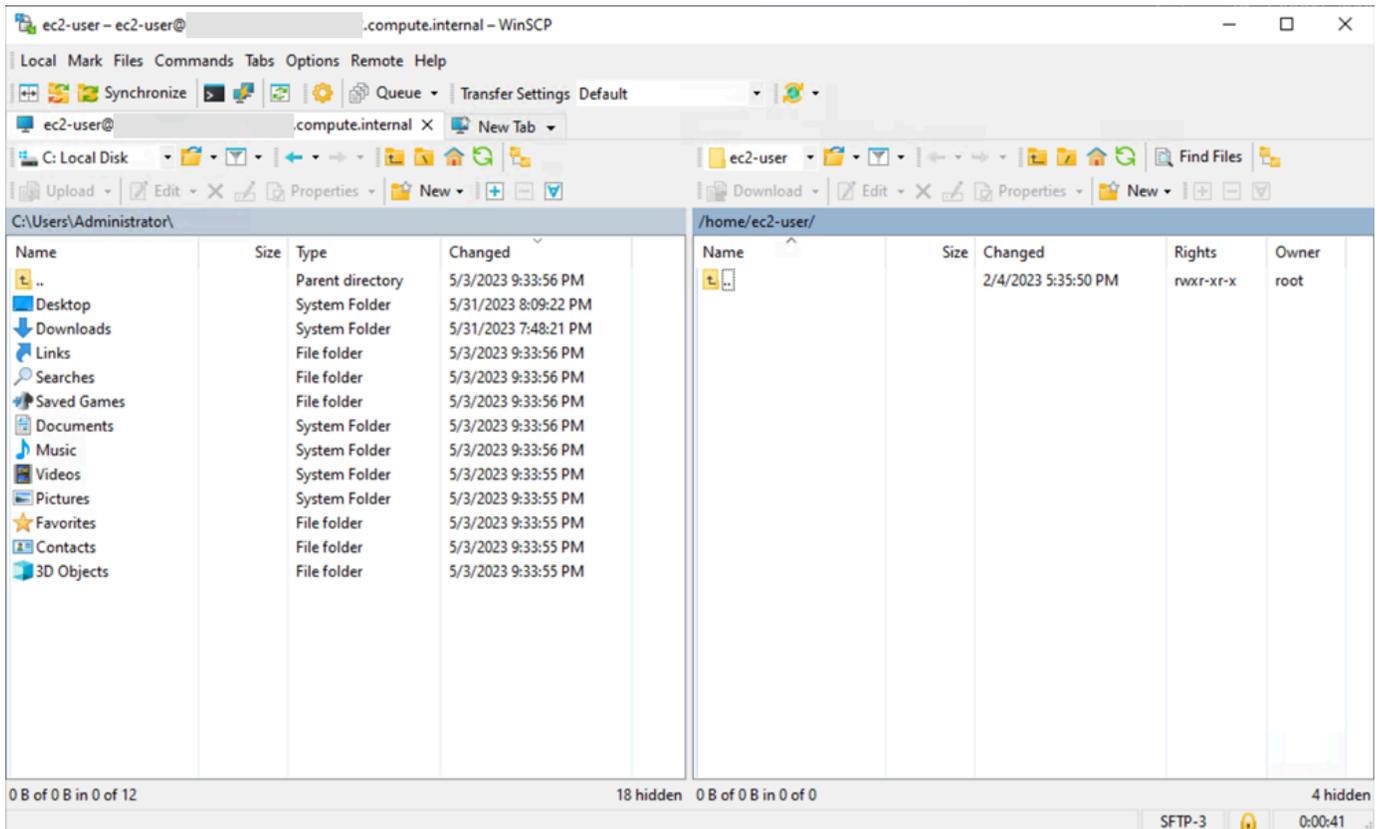
5. Spécifiez le fichier de clé privée pour votre instance.
- a. Choisissez le bouton Avancé....
 - b. Sous SSH, choisissez Authentification.
 - c. Spécifiez le chemin d'accès de votre fichier de clé privée, ou cliquez sur le bouton ... pour rechercher le fichier de paire de clés.
 - d. Choisissez OK.

Voici une capture d'écran de WinSCP version 6.1 :



WinSCP a besoin d'un fichier clé privé PuTTY (.ppk). Vous pouvez convertir un fichier de clé de sécurité .pem au format .ppk à l'aide de PuTTYgen. Pour plus d'informations, consultez [Convertir votre clé privée avec PuTTYgen](#).

6. (Facultatif) Dans le volet gauche, choisissez Directories (Répertoires). Pour Remote directory (Répertoire distant), entrez le chemin d'accès du répertoire auquel ajouter les fichiers. Pour ouvrir les paramètres de site avancés, pour les versions les plus récentes de WinSCP, choisissez Advanced (Avancé). Pour rechercher le paramètre Remote directory (Répertoire distant), sous Environment (Environnement), choisissez Directories (Répertoires).
7. Choisissez Login (Connexion). Pour ajouter l'empreinte hôte au cache hôte, choisissez Yes (Oui).



8. Une fois que la connexion est établie, dans la fenêtre de connexion, votre instance Linux est à droite et votre machine locale est à gauche. Vous pouvez glisser-déposer des fichiers entre le système de fichiers distant et votre ordinateur local. Pour obtenir plus d'information sur WinSCP, consultez la documentation du projet sur <http://winscp.net/eng/docs/start>.

Si vous recevez une erreur indiquant que vous ne pouvez pas exécuter SCP pour démarrer le transfert, vérifiez que vous avez installé `scp` sur l'instance Linux.

Connexion à vos instances Linux à partir de Windows à l'aide du sous-système Windows pour Linux (WSL)

Après avoir lancé votre instance, vous pouvez connecter à celle-ci et l'utiliser comme vous le feriez d'un ordinateur devant lequel vous seriez assis.

Les instructions suivantes expliquent comment vous connecter à votre instance à l'aide d'une distribution Linux sur le sous-système Windows pour Linux (WSL). WSL est en téléchargement gratuit et vous permet d'exécuter des outils de ligne de commande Linux natifs directement sur Windows, avec votre bureau Windows traditionnel, sans la surcharge d'une machine virtuelle.

En installant WSL, vous pouvez utiliser un environnement Linux natif pour vous connecter à vos instances Linux EC2 au lieu de faire appel à PuTTY ou PuTTYgen. L'environnement Linux vous permet de vous connecter à vos instances Linux plus facilement, car il comprend un client SSH natif que vous pouvez utiliser pour vous connecter à vos instances Linux et pour modifier les autorisations du fichier de clé .pem. La console Amazon EC2 fournit la commande SSH pour se connecter à l'instance Linux, et vous pouvez obtenir des informations plus détaillées à partir de la commande SSH pour le dépannage. Pour plus d'informations, consultez la [documentation Windows Subsystem pour Linux](#).

Note

Une fois que vous avez installé WSL, tous les prérequis et les étapes sont les mêmes que ceux décrits dans [Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#), et vous bénéficiez d'une expérience similaire à l'utilisation de Linux natif.

Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [Résoudre les problèmes de connexion à votre instance Linux](#).

Table des matières

- [Prérequis](#)
- [Se connecter à votre instance Linux avec WSL](#)
- [Transfert de fichiers vers des instances Linux à partir de Linux à l'aide de SCP](#)
- [Désinstaller WSL](#)

Prérequis

Avant de vous connecter à votre instance Linux, remplissez les prérequis suivants.

Vérifiez que l'instance est prête.

Une fois l'instance lancée, il peut falloir quelques minutes pour qu'elle soit prête pour que vous puissiez vous y connecter. Vérifiez que votre instance a réussi les contrôles de statut. Vous pouvez afficher ces informations dans la colonne Status check (Vérification de statut) de la page instances.

Vérifiez les prérequis généraux pour la connexion à votre instance.

Pour rechercher le nom DNS public ou l'adresse IP de votre instance et le nom d'utilisateur que vous devez utiliser pour vous connecter à cette dernière, consultez [Obtenez des informations sur votre instance](#).

Installez Windows Subsystem for Linux (WSL) et une distribution Linux sur votre ordinateur local.

Installez WSL et une distribution Linux à l'aide des instructions du [Guide d'installation de Windows 10](#). L'exemple des instructions installe la distribution Ubuntu de Linux, mais vous pouvez installer n'importe quelle distribution. Vous êtes invité à redémarrer votre ordinateur pour que les modifications prennent effet.

Copiez la clé privée depuis Windows vers WSL

Dans une fenêtre de terminal WSL, copiez le fichier `.pem` (pour la paire de clés que vous avez spécifiée lorsque vous avez lancé l'instance) de Windows vers WSL. Notez le chemin d'accès qualifié complet vers le fichier `.pem` sur WSL à utiliser lors de la connexion à votre instance. Pour plus d'informations sur la façon de spécifier le chemin vers votre disque dur Windows, consultez [How do I access my C drive ?](#). Pour plus d'informations sur les paires de clés et les instances Windows, consultez [Paires de clés Amazon EC2 et instances Windows](#).

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

Se connecter à votre instance Linux avec WSL

Utilisez la procédure suivante pour vous connecter à votre instance Linux à l'aide de Windows Subsystem pour Linux (WSL). Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [Résoudre les problèmes de connexion à votre instance Linux](#).

Pour vous connecter à votre instance à l'aide de SSH

1. Utilisez la commande `ssh` dans une fenêtre de terminal pour vous connecter à l'instance. Vous spécifiez le chemin et le nom de fichier de la clé privée (`.pem`), le nom d'utilisateur de votre AMI et le nom DNS public ou l'adresse IPv6 de votre instance. Pour savoir comment trouver la clé privée, le nom d'utilisateur d'une instance et le nom DNS ou l'adresse IPv6 d'une instance, consultez [Localisation de la clé privée et définition des autorisations](#) et [Obtenez des informations sur votre instance](#). Pour vous connecter à votre instance, utilisez l'une des commandes suivantes.

- (DNS public) Pour vous connecter à l'aide du nom DNS public de votre instance, entrez la commande suivante.

```
ssh -i /path/key-pair-name.pem instance-user-name@my-instance-public-dns-name
```

- (IPv6) Sinon, si votre instance possède une adresse IPv6, vous pouvez vous connecter à l'instance à l'aide de son adresse IPv6. Spécifiez la commande ssh avec le chemin d'accès au fichier de clé privée (.pem), le nom d'utilisateur approprié et l'adresse IPv6.

```
ssh -i /path/key-pair-name.pem instance-user-name@my-instance-IPv6-address
```

Vous verrez une réponse telle que celle ci-après:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

2. (Facultatif) Vérifiez que l'empreinte de l'alerte de sécurité correspond à l'empreinte que vous avez précédemment obtenue dans [\(Facultatif\) Obtenez l'empreinte digitale de l'instance](#). Si ces empreintes ne correspondent pas, quelqu'un essaie peut-être d'effectuer une attaque MITM. Si elles correspondent, passez à l'étape suivante.
3. Saisissez yes.

Vous verrez une réponse telle que celle ci-après:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
```

Transfert de fichiers vers des instances Linux à partir de Linux à l'aide de SCP

Le transfert de fichiers entre votre ordinateur local et une instance Linux peut se faire en le protocole de copie sécurisée (SCP). Cette section décrit comment transférer des fichiers avec SCP. La procédure est similaire à celle de la connexion à une instance avec SSH.

Prérequis

- Vérifiez les prérequis généraux pour le transfert de fichiers à votre instance.

Avant de transférer des fichiers entre votre ordinateur local et votre instance, effectuez les actions suivantes pour vous assurer que vous disposez de toutes les informations dont vous avez besoin.

- [Obtenez des informations sur votre instance](#)
- [Localisation de la clé privée et définition des autorisations](#)
- [\(Facultatif\) Obtenez l’empreinte digitale de l’instance](#)
- Installez un client SCP

La plupart des ordinateurs Linux, Unix et Apple comporte un client SCP par défaut. Si ce n’est pas le cas pour le vôtre, le projet OpenSSH offre une implémentation gratuite de l’ensemble de la suite d’outils SSH, notamment un client SCP. Pour plus d’informations, consultez <https://www.openssh.com>.

La procédure suivante vous guide pour le transfert d’un fichier avec SCP. Si vous êtes déjà connecté à l’instance avec SSH et que vous avez vérifié ses empreintes, vous pouvez commencer l’étape qui contient la commande SCP (étape 4).

Pour utiliser SCP pour transférer un fichier

1. Transférez un fichier vers votre instance à l’aide du nom DNS public de l’instance. Par exemple, si le nom du fichier clé privé est `key-pair-name`, le fichier à transférer est `SampleFile.txt`, le nom d’utilisateur est `instance-user-name` et le nom DNS public de l’instance est `my-instance-public-dns-name` ou l’adresse IPv6 est `my-instance-IPv6-address`, utilisez la commande suivante pour copier le fichier dans le répertoire de base `instance-user-name`.
 - (DNS public) Pour transférer un fichier à l’aide du nom DNS public de votre instance, entrez la commande suivante.

```
scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@my-instance-public-dns-name:~
```

- (IPv6) Sinon, si votre instance possède une adresse IPv6, vous pouvez transférer un fichier à l’aide de l’adresse IPv6 de l’instance. L’adresse IPv6 doit être placée entre crochets (`[]`), lesquels doivent être précédés d’un caractère d’échappement (`\`).

```
scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@[my-instance-IPv6-address]:~
```

Vous verrez une réponse telle que celle ci-après:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

- (Facultatif) Vérifiez que l'empreinte de l'alerte de sécurité correspond à l'empreinte que vous avez précédemment obtenue dans [\(Facultatif\) Obtenez l'empreinte digitale de l'instance](#). Si ces empreintes ne correspondent pas, quelqu'un essaie peut-être d'effectuer une attaque MITM. Si elles correspondent, passez à l'étape suivante.
- Saisissez **yes**.

Vous verrez une réponse telle que celle ci-après:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
Sending file modes: C0644 20 SampleFile.txt
Sink: C0644 20 SampleFile.txt
SampleFile.txt                               100%   20    0.0KB/s   00:00
```

Si l'erreur « bash: scp: command not found » s'affiche, vous devez d'abord installer scp sur votre instance Linux. Pour certains systèmes d'exploitation, elle se trouve dans le package `openssh-clients`. Pour les variantes Amazon Linux comme l'AMI optimisée pour Amazon ECS, utilisez la commande suivante pour installer scp :

```
[ec2-user ~]$ sudo yum install -y openssh-clients
```

- Pour transférer les fichiers dans l'autre direction (de votre instance Amazon EC2 à votre ordinateur local), inversez l'ordre des paramètres de l'hôte. Par exemple, pour retransférer le fichier `SampleFile.txt` depuis votre instance EC2 vers le répertoire de base de votre ordinateur local en tant que `SampleFile2.txt`, utilisez l'une des commandes suivantes sur votre ordinateur local.
 - (DNS public) Pour transférer un fichier à l'aide du nom DNS public de votre instance, entrez la commande suivante.

```
scp -i /path/key-pair-name.pem instance-user-  
name@ec2-198-51-100-1.compute-1.amazonaws.com:~/SampleFile.txt ~/  
SampleFile2.txt
```

- (IPv6) Sinon, si votre instance possède une adresse IPv6, pour transférer des fichiers dans l'autre sens à l'aide de l'adresse IPv6 de l'instance, entrez la commande suivante.

```
scp -i /path/key-pair-name.pem instance-user-name@  
\[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~/SampleFile.txt ~/SampleFile2.txt
```

Désinstaller WSL

Pour plus d'informations sur la façon de désinstaller Windows Subsystem pour Linux, consultez [How do I uninstall a WSL Distribution ?](#).

Connexion à votre instance Linux avec EC2 Instance Connect

Amazon EC2 Instance Connect vous fournit une solution simple et sécurisée pour vous connecter à vos instances Linux à l'aide de Secure Shell (SSH). Avec EC2 Instance Connect, vous utilisez des [politiques](#) et des [principes AWS Identity and Access Management \(IAM\)](#) pour contrôler l'accès SSH à vos instances, éliminant ainsi le besoin de partager et de gérer les clés SSH. Toutes les demandes de connexion utilisant EC2 Instance Connect sont [enregistrées afin que vous AWS CloudTrail puissiez auditer les demandes de connexion](#).

Vous pouvez utiliser EC2 Instance Connect pour vous connecter à vos instances à l'aide de la console Amazon EC2 ou d'un client SSH de votre choix.

Lorsque vous vous connectez à une instance à l'aide d'EC2 Instance Connect, l'API Instance Connect envoie en mode push une clé publique SSH vers les [métadonnées de l'instance](#), où elle demeure pendant 60 secondes. La politique IAM attachée à votre utilisateur l'autorise à envoyer en mode push la clé publique vers les métadonnées de l'instance. Le démon SSH utilise `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser`, qui sont configurés lors de l'installation d'Instance Connect, pour rechercher la clé publique à partir des métadonnées de l'instance en vue de son authentification, et vous connecte à l'instance.

Vous pouvez utiliser EC2 Instance Connect pour vous connecter à des instances qui ont des adresses IP publiques ou privées. Pour plus d'informations, consultez [Connexion à l'aide de EC2 Instance Connect](#).

Pour un article de blog qui explique comment améliorer la sécurité de vos hôtes bastion à l'aide d'EC2 Instance Connect, consultez [Securing your bastion hosts with Amazon EC2 Instance Connect](#) (français non garanti).

 Tip

EC2 Instance Connect est l'une des options de connexion à votre instance Linux. Pour d'autres options, veuillez consulter la rubrique [Connectez-vous à votre instance Linux](#). Pour vous connecter à une instance Windows, consultez [Connexion à votre instance Windows](#).

Table des matières

- [Tutoriel : complétez la configuration requise pour vous connecter à votre instance à l'aide d'EC2 Instance Connect](#)
- [Prérequis](#)
- [Accorder des autorisations IAM pour EC2 Instance Connect](#)
- [Installer EC2 Instance Connect sur vos instances EC2](#)
- [Connexion à l'aide de EC2 Instance Connect](#)
- [Désinstallation d'EC2 Instance Connect](#)

Tutoriel : complétez la configuration requise pour vous connecter à votre instance à l'aide d'EC2 Instance Connect

Pour vous connecter à votre instance à l'aide d'EC2 Instance Connect dans la console Amazon EC2, vous devez d'abord effectuer la configuration préalable qui vous permettra de vous connecter correctement à votre instance. Le but de ce didacticiel est de vous guider à travers les tâches nécessaires à la réalisation de la configuration préalable.

Aperçu du didacticiel

Dans ce didacticiel, vous allez effectuer les quatre tâches suivantes :

- [Tâche 1 : créer et joindre une politique IAM pour vous permettre d'utiliser EC2 Instance Connect](#)

Vous allez d'abord créer une politique IAM contenant les autorisations IAM qui vous permettent d'envoyer une clé publique aux métadonnées de l'instance. Vous allez associer cette politique à votre identité IAM (utilisateur, groupe d'utilisateurs ou rôle) afin que votre identité IAM obtienne ces autorisations.

- [Tâche 2 : créer un groupe de sécurité pour autoriser le trafic entrant du service EC2 Instance Connect vers votre instance](#)

Vous allez ensuite créer un groupe de sécurité qui autorise le trafic du service EC2 Instance Connect vers votre instance. Cela est nécessaire lorsque vous utilisez EC2 Instance Connect dans la console Amazon EC2 pour vous connecter à votre instance.

- [Tâche 3 : Lancer votre instance](#)

Vous lancerez ensuite une instance EC2 à l'aide d'une AMI préinstallée avec EC2 Instance Connect et vous ajouterez le groupe de sécurité que vous avez créé à l'étape précédente.

- [Tâche 4 : Se connecter à votre instance](#)

Enfin, vous utiliserez EC2 Instance Connect dans la console Amazon EC2 pour vous connecter à votre instance. Si vous pouvez vous connecter, vous pouvez être sûr que la configuration préalable que vous avez effectuée dans les tâches 1, 2 et 3 a été effectuée avec succès.

Tâche 1 : créer et joindre une politique IAM pour vous permettre d'utiliser EC2 Instance Connect

Lorsque vous vous connectez à une instance à l'aide d'EC2 Instance Connect, l'API EC2 Instance Connect envoie en mode push une clé publique SSH vers les [métadonnées de l'instance](#), où elle demeure pendant 60 secondes. Vous avez besoin d'une politique IAM associée à votre identité IAM (utilisateur, groupe d'utilisateurs ou rôle) pour vous accorder l'autorisation requise pour transmettre la clé publique aux métadonnées de l'instance.

Objectif de la tâche

Dans cette tâche, vous allez créer la politique IAM qui autorise l'envoi de la clé publique à l'instance. L'action spécifique à autoriser est `ec2-instance-connect:SendSSHPublicKey`. Vous devez également autoriser `ec2:DescribeInstances` afin de pouvoir afficher et sélectionner votre instance dans la console Amazon EC2.

Une fois que vous avez créé la politique, vous l'associez à votre identité IAM (utilisateur, groupe d'utilisateurs ou rôle) afin que votre identité IAM obtienne les autorisations.

Vous allez créer une politique configurée comme suit :

```
{
  "Version": "2012-10-17",
  "Statement": [{
```

```
    "Effect": "Allow",
    "Action": "ec2-instance-connect:SendSSHPublicKey",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:DescribeInstances",
    "Resource": "*"
  }
]
```

Important

La politique IAM créée dans ce didacticiel est une politique hautement permissive ; elle vous permet de vous connecter à n'importe quelle instance en utilisant n'importe quel nom d'utilisateur AMI. Nous utilisons cette politique hautement permissive pour que le didacticiel reste simple et se concentre sur les configurations spécifiques enseignées dans ce didacticiel. Toutefois, dans un environnement de production, nous vous recommandons de configurer votre politique IAM de manière à fournir des autorisations de [moindre privilège](#). Par exemple les stratégies IAM, consultez [Accorder des autorisations IAM pour EC2 Instance Connect](#).

Étapes pour créer et associer la politique IAM

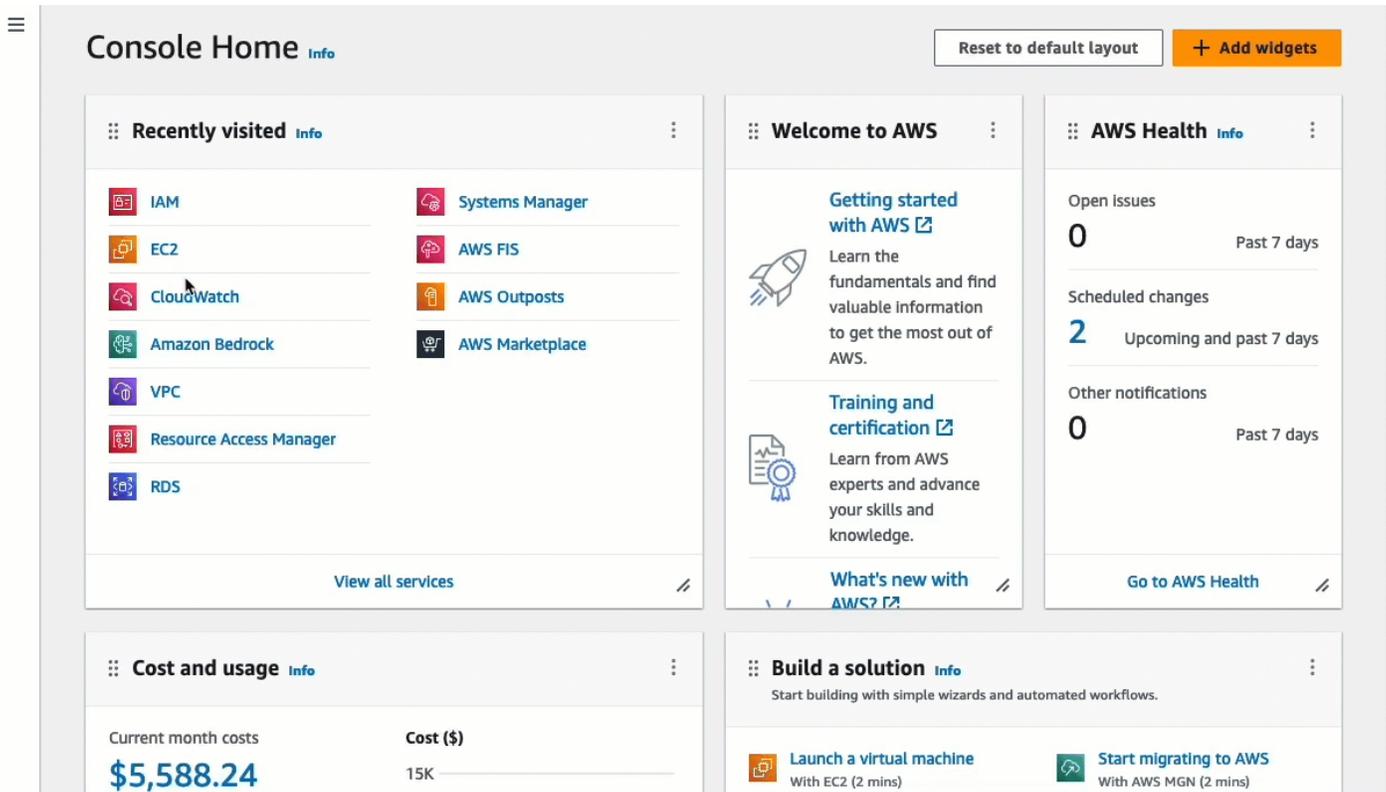
Suivez les étapes ci-dessous pour créer et associer la politique IAM. Pour afficher une animation des étapes, reportez-vous aux sections [Afficher une animation : créer une politique IAM](#) et [Afficher une animation : joindre une politique IAM](#).

Pour créer et associer une politique IAM vous permettant d'utiliser EC2 Instance Connect pour vous connecter à vos instances

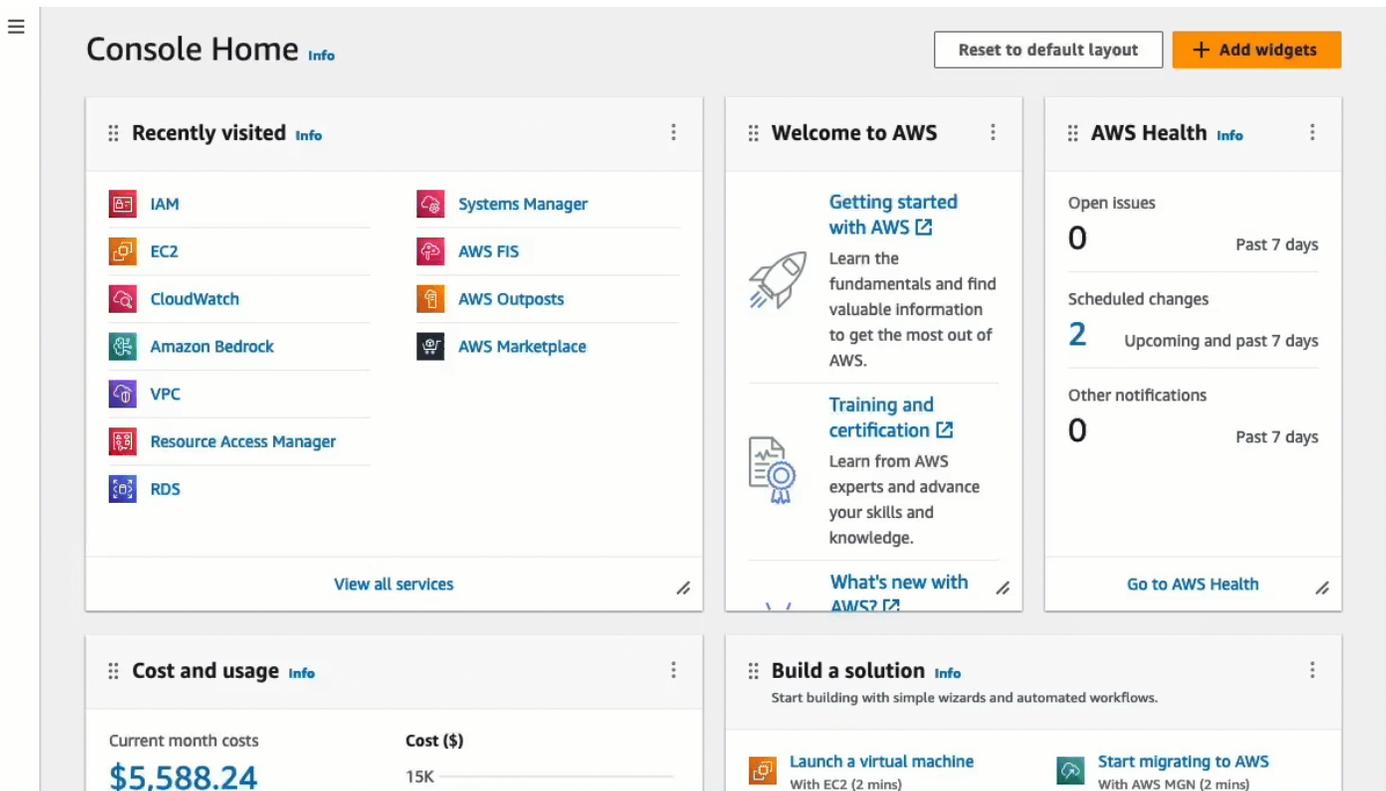
1. Créez d'abord la politique IAM
 - a. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
 - b. Dans le panneau de navigation, choisissez Politiques (Politiques).
 - c. Sélectionnez Create policy (Créer une politique).
 - d. Sur la page Spécifier l'autorisation, procédez comme suit :

- i. Pour Service, choisissez EC2 Instance Connect.
 - ii. Sous Actions autorisées, dans le champ de recherche, commencez **send** à taper pour afficher les actions pertinentes, puis sélectionnez SendSSH PublicKey.
 - iii. Sous Ressources, sélectionnez Tout. Pour un environnement de production, nous recommandons de spécifier l'instance par son ARN, mais pour ce didacticiel, vous autorisez toutes les instances.
 - iv. Choisissez Ajouter d'autres autorisations.
 - v. Pour Service, choisissez EC2.
 - vi. Sous Actions autorisées, dans le champ de recherche, commencez **describein** à taper pour afficher les actions pertinentes, puis sélectionnez DescribeInstances.
 - vii. Choisissez Suivant.
- e. Sur la page Réviser et créer, procédez comme suit :
 - i. Pour Policy name (Nom de la stratégie), attribuez un nom à cette stratégie.
 - ii. Choisissez Créer une politique.
2. Attachez ensuite la politique à votre identité
 - a. Dans le panneau de navigation de la console IAM, sélectionnez Politiques (Politiques).
 - b. Dans la liste des politiques, sélectionnez le bouton d'option à côté du nom de la politique que vous avez créée. Vous pouvez utiliser la zone de recherche pour filtrer la liste des politiques.
 - c. Sélectionnez Actions, puis Attach (Attacher).
 - d. Sous Entités IAM, cochez la case à côté de votre identité (utilisateur, groupe d'utilisateurs ou rôle). Vous pouvez utiliser le champ de recherche pour filtrer la liste des entités.
 - e. Choisissez Attach policy (Attacher une politique).

Afficher une animation : créer une politique IAM



Afficher une animation : joindre une politique IAM



Tâche 2 : créer un groupe de sécurité pour autoriser le trafic entrant du service EC2 Instance Connect vers votre instance

Lorsque vous utilisez EC2 Instance Connect dans la console Amazon EC2 pour vous connecter à une instance, le trafic qui doit être autorisé à atteindre l'instance est le trafic provenant du service EC2 Instance Connect. Cela est différent de la connexion de votre ordinateur local à une instance ; dans ce cas, vous devez autoriser le trafic entre votre ordinateur local et votre instance. Pour autoriser le trafic provenant du service EC2 Instance Connect, vous devez créer un groupe de sécurité qui autorise le trafic SSH entrant depuis la plage d'adresses IP du service EC2 Instance Connect.

Les plages d'adresses IP des AWS services sont disponibles sur <https://ip-ranges.amazonaws.com/ip-ranges.json>. Les plages d'adresses IP d'EC2 Instance Connect sont identifiées par "service" : "EC2_INSTANCE_CONNECT".

Objectif de la tâche

Dans cette tâche, vous trouverez d'abord la plage d'adresses IP EC2_INSTANCE_CONNECT Région AWS dans laquelle se trouve votre instance. Vous allez ensuite créer un groupe de sécurité qui autorise le trafic SSH entrant sur le port 22 à partir de cette plage d'adresses IP.

Étapes de création du groupe de sécurité

Procédez comme suit pour créer le groupe de sécurité. Pour afficher une animation des étapes, reportez-vous aux sections [Afficher une animation : obtenir la plage d'adresses IP pour EC2 Instance Connect pour une région spécifique](#) et [Afficher une animation : Configuration d'un groupe de sécurité](#).

Pour créer un groupe de sécurité qui autorise le trafic entrant du service EC2 Instance Connect vers votre instance

1. Obtenez d'abord la plage d'adresses IP pour le service EC2 Instance Connect
 - a. Ouvrez le fichier JSON des plages d'adresses AWS IP à l'[adresse https://ip-ranges.amazonaws.com/ip-ranges.json](https://ip-ranges.amazonaws.com/ip-ranges.json).
 - b. Choisissez Raw Data.
 - c. Trouvez la plage d'adresses IP correspondant EC2_INSTANCE_CONNECT à celle Région AWS dans laquelle se trouve votre instance. Vous pouvez utiliser le champ de recherche du navigateur pour rechercher le service EC2_INSTANCE_CONNECT et poursuivre votre recherche jusqu'à ce que vous trouviez la région dans laquelle se trouve votre instance.

Par exemple, si votre instance est située dans la région USA Est (Virginie du Nordus-east-1) (), la plage d'adresses IP pour EC2_INSTANCE_CONNECT cette région est 18.206.107.24/29.

 Note

Les plages d'adresses IP sont différentes pour chacune d'entre elles Région AWS.

- d. Copiez la plage d'adresses IP qui apparaît à côté de `deip_prefix`. Vous utiliserez cette plage d'adresses IP ultérieurement dans cette procédure.

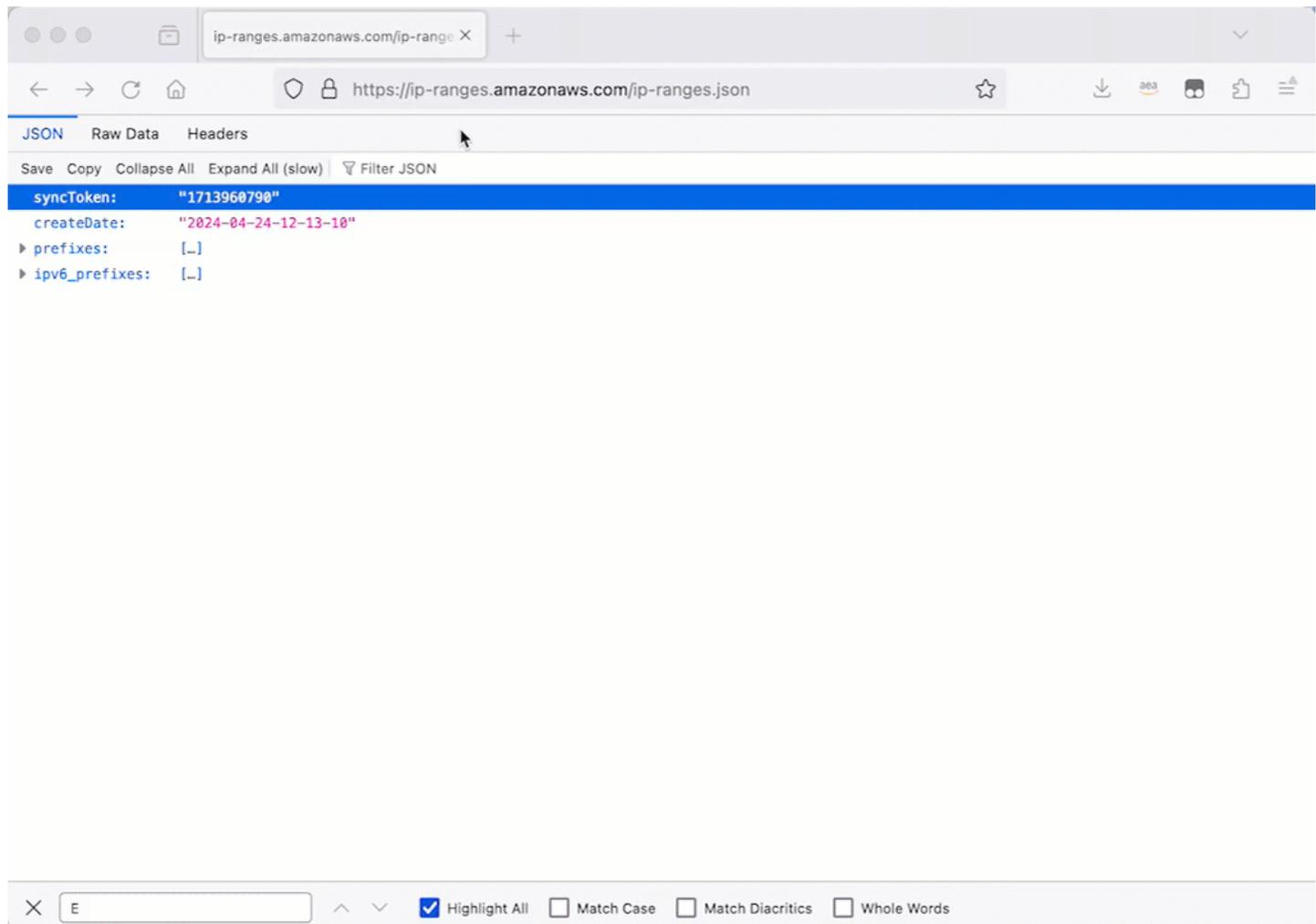
Pour plus d'informations sur le téléchargement du fichier JSON des plages d'adresses AWS IP et le filtrage par service, consultez la section [Plages d'adresses AWS IP](#) dans le guide de l'utilisateur Amazon VPC.

2. Créez ensuite le groupe de sécurité avec une règle entrante pour autoriser le trafic provenant de la plage d'adresses IP copiée.
 - a. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
 - b. Dans le panneau de navigation, choisissez Groupes de sécurité.
 - c. Sélectionnez Create security group (Créer un groupe de sécurité).
 - d. Sous Basic details (Détails de base), procédez comme suit :
 - i. Dans Nom du groupe de sécurité, entrez un nom significatif pour votre groupe de sécurité.
 - ii. Dans Description, entrez une description significative pour votre groupe de sécurité.
 - e. Sous Règles de trafic entrant, procédez comme suit :
 - i. Choisissez Ajouter une règle.
 - ii. Pour Type, choisissez SSH.
 - iii. Pour Source, laissez Personnalisé.
 - iv. Dans le champ situé à côté de Source, collez la plage d'adresses IP du service EC2 Instance Connect que vous avez copiée plus tôt dans cette procédure.

Par exemple, si votre instance est située dans la région USA Est (Virginie du Nord) (us-east-1), collez la plage d'adresses IP suivante dans le champ :
18.206.107.24/29

- f. Sélectionnez Create security group (Créer un groupe de sécurité).

Afficher une animation : obtenir la plage d'adresses IP pour EC2 Instance Connect pour une région spécifique

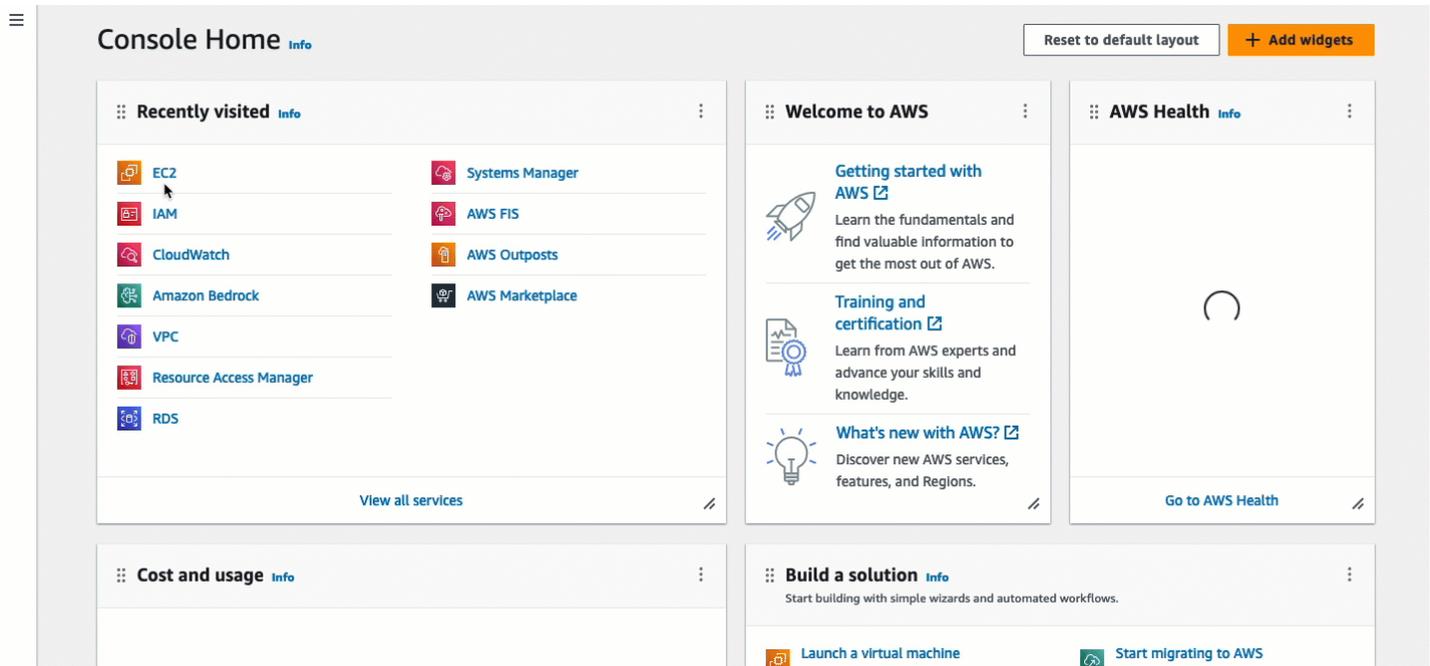


The screenshot shows a web browser window with the URL `https://ip-ranges.amazonaws.com/ip-ranges.json`. The browser's developer tools are open to the JSON tab, displaying the following response:

```
{
  "syncToken": "1713960790",
  "createDate": "2024-04-24-12-13-10",
  "prefixes": [],
  "ipv6_prefixes": []
}
```

Below the JSON response, there is a search bar with the letter 'E' entered. The search options are: Highlight All, Match Case, Match Diacritics, and Whole Words.

Afficher une animation : Configuration d'un groupe de sécurité



Tâche 3 : Lancer votre instance

Lorsque vous lancez une instance, vous devez spécifier une AMI contenant les informations requises pour lancer l'instance. Vous pouvez choisir de lancer une instance avec ou sans EC2 Instance Connect préinstallé. Dans cette tâche, nous indiquons une AMI préinstallée avec EC2 Instance Connect.

Si vous lancez votre instance sans EC2 Instance Connect préinstallé et que vous souhaitez utiliser EC2 Instance Connect pour vous connecter à votre instance, vous devrez effectuer des étapes de configuration supplémentaires. Ces étapes n'entrent pas dans le cadre de ce didacticiel.

Objectif de la tâche

Dans cette tâche, vous allez lancer une instance avec l'AMI Amazon Linux 2023, qui est préinstallée avec EC2 Instance Connect. Vous allez également spécifier le groupe de sécurité que vous avez créé précédemment afin de pouvoir utiliser EC2 Instance Connect dans la console Amazon EC2 pour vous connecter à votre instance. Comme vous utiliserez EC2 Instance Connect pour vous connecter à votre instance, ce qui envoie une clé publique aux métadonnées de votre instance, vous n'aurez pas besoin de spécifier de clé SSH lorsque vous lancerez votre instance. Cependant, vous devez vous assurer que votre instance possède une adresse IPv4 publique, car l'utilisation d'EC2 Instance Connect dans la console Amazon EC2 permet de se connecter uniquement aux instances dotées d'adresses IPv4 publiques.

Étapes pour lancer votre instance

Suivez les étapes ci-dessous pour lancer votre instance. Pour visionner une animation des étapes, voir [Afficher une animation : lancez votre instance](#).

Pour lancer une instance qui peut utiliser EC2 Instance Connect dans la console Amazon EC2 pour la connexion

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation en haut de l'écran, la AWS région actuelle est affichée (par exemple, l'Irlande). Sélectionnez la région dans laquelle vous souhaitez lancer votre instance. Ce choix est important car vous avez créé un groupe de sécurité qui autorise le trafic pour une région spécifique. Vous devez donc sélectionner la même région dans laquelle lancer votre instance.
3. Sur le tableau de bord de la console Amazon EC2, sélectionnez Launch instance (Lancer une instance).
4. (Facultatif) Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom descriptif pour votre instance.
5. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), choisissez Quick Start. Amazon Linux est sélectionné par défaut. Sous Amazon Machine Image (AMI), l'AMI Amazon Linux 2023 est sélectionnée par défaut. Conservez la sélection par défaut pour cette tâche.
6. Sous Type d'instance, pour Type d'instance, conservez la sélection par défaut ou choisissez un autre type d'instance.
7. Sous Paire de clés (connexion), pour Nom de la paire de clés, choisissez Procéder sans paire de clés (Non recommandé). Lorsque vous utilisez EC2 Instance Connect pour vous connecter à une instance, EC2 Instance Connect envoie une paire de clés aux métadonnées de l'instance, et c'est cette paire de clés qui est utilisée pour la connexion.
8. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :
 - a. Pour Attribuer automatiquement une adresse IP publique, laissez Activer.

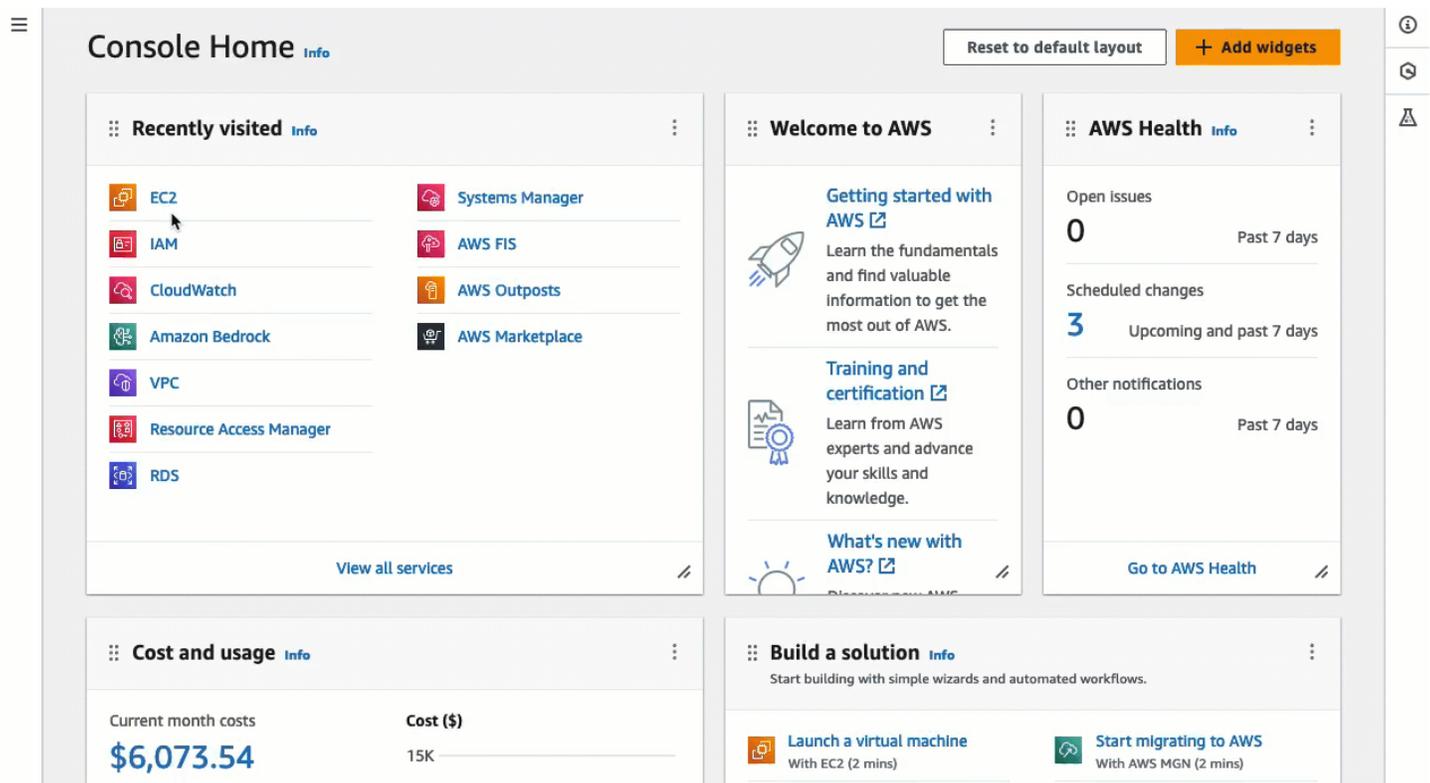
Note

Pour utiliser EC2 Instance Connect dans la console Amazon EC2 afin de se connecter à une instance, celle-ci doit disposer d'une adresse IPv4 publique.

- b. Pour Pare-feu (groupes de sécurité), choisissez Sélectionner un groupe de sécurité existant.

- c. Sous Groupes de sécurité communs, choisissez le groupe de sécurité que vous avez créé précédemment.
9. Dans le panneau Summary (Récapitulatif), sélectionnez Launch instance (Lancer l'instance).

Afficher une animation : lancez votre instance



Tâche 4 : Se connecter à votre instance

Lorsque vous vous connectez à une instance à l'aide d'EC2 Instance Connect, l'API EC2 Instance Connect envoie en mode push une clé publique SSH vers les [métadonnées de l'instance](#), où elle demeure pendant 60 secondes. Le démon SSH utilise `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser` pour rechercher la clé publique dans les métadonnées de l'instance à des fins d'authentification, et vous connecte à l'instance.

Objectif de la tâche

Dans cette tâche, vous allez vous connecter à votre instance à l'aide d'EC2 Instance Connect dans la console Amazon EC2. Si vous avez effectué les tâches 1, 2 et 3 requises, la connexion devrait réussir.

Étapes pour vous connecter à votre instance

Suivez les étapes ci-dessous pour vous connecter à votre instance. Pour visionner une animation des étapes, voir [Afficher une animation : Connectez-vous à votre instance](#).

Pour connecter une instance à l'aide d'EC2 Instance Connect dans la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation en haut de l'écran, la AWS région actuelle est affichée (par exemple, l'Irlande). Sélectionnez la région dans laquelle se trouve votre instance.
3. Dans le panneau de navigation, sélectionnez Instances.
4. Sélectionnez votre instance, puis choisissez Connect.
5. Choisissez l'onglet EC2 Instance Connect.
6. Pour le type de connexion, choisissez Connect using EC2 Instance Connect.
7. Choisissez Se connecter.

Une fenêtre de terminal s'ouvre dans le navigateur et vous êtes connecté à votre instance.

Afficher une animation : Connectez-vous à votre instance

The screenshot displays the AWS Management Console Home page. At the top, there's a navigation bar with 'Console Home' and a 'Reset to default layout' button. Below this, the page is organized into several sections:

- Recently visited:** A grid of service tiles including EC2, IAM, CloudWatch, Amazon Bedrock, VPC, Resource Access Manager, RDS, Systems Manager, AWS FIS, AWS Outposts, and AWS Marketplace. A 'View all services' link is at the bottom.
- Welcome to AWS:** A section with three cards: 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'. Each card includes a brief description and a link to learn more.
- AWS Health:** A section showing 'Open issues' (0), 'Scheduled changes' (3), and 'Other notifications' (0) for the past 7 days. A 'Go to AWS Health' link is at the bottom.
- Cost and usage:** A section showing 'Current month costs' of \$6,073.54, which is a 3% decrease compared to the last month for the same period. A bar chart shows costs up to 15K.
- Build a solution:** A section with four cards: 'Launch a virtual machine', 'Register a domain', 'Start migrating to AWS', and 'Host a static web app'. Each card includes a brief description and a link to learn more.

Prérequis

Les conditions préalables à l'installation d'EC2 Instance Connect et à l'utilisation d'EC2 Instance Connect pour se connecter à une instance sont les suivantes :

- [Régions AWS](#)
- [Zones locales](#)
- [AMI](#)
- [Installation d'EC2 Instance Connect](#)
- [IPv4 address \(Adresse IPv4\)](#)
- [Accès réseau](#)
- [Règle de groupe de sécurité](#)
- [Accorder des autorisations](#)
- [Configuration de l'ordinateur local](#)
- [Nom d'utilisateur](#)

Régions AWS

Pris en charge partout Régions AWS sauf dans le Canada-Ouest (Calgary).

Zones locales

Non pris en charge.

AMI

EC2 Instance Connect est préinstallé sur les AMI suivantes :

- AL2023
- Amazon Linux 2 2.0.20190618 ou version ultérieure
- macOS Sonoma 14.2.1 ou version ultérieure
- macOS Ventura 13.6.3 ou version ultérieure
- macOS Monterey 12.7.2 ou version ultérieure
- Ubuntu 20.04 ou version ultérieure

EC2 Instance Connect n'est pas préinstallé sur les AMI suivantes, mais vous pouvez l'installer sur des instances lancées à l'aide des AMI suivantes :

- Amazon Linux 2 avant la version 2.0.20190618
- CentOS Stream 8 et 9
- macOS Sonoma avant 14.2.1, Ventura avant 13.6.3 et Monterey avant 12.7.2
- Red Hat Enterprise Linux (RHEL) 8 et 9
- Ubuntu 16.04 et 18.04

Installation d'EC2 Instance Connect

Pour utiliser EC2 Instance Connect afin de se connecter à une instance, EC2 Instance Connect doit être installé sur celle-ci. Vous pouvez soit lancer l'instance à l'aide d'une AMI préinstallée avec EC2 Instance Connect, soit installer EC2 Instance Connect sur des instances lancées avec des AMI prises en charge. Pour connaître les AMI prises en charge, reportez-vous à la section précédente. Pour les instructions d'installation, consultez [Installer EC2 Instance Connect sur vos instances EC2](#).

IPv4 address (Adresse IPv4)

Votre instance doit avoir une adresse IPv4 (privée ou publique). EC2 Instance Connect ne prend pas en charge la connexion à l'aide d'une adresse IPv6.

Accès réseau

Les instances peuvent être configurées pour permettre aux utilisateurs de se connecter à votre instance via Internet ou via l'adresse IP privée de l'instance. En fonction de la façon dont vos utilisateurs se connecteront à votre instance en utilisant EC2 Instance Connect, vous devez configurer l'accès réseau suivant :

- Si vos utilisateurs se connecteront à votre instance via internet, votre instance doit alors avoir une adresse IP publique et se trouver dans un sous-réseau public. Pour plus d'informations, consultez [Activer l'accès à Internet](#) dans le Guide de l'utilisateur Amazon VPC.
- Si vos utilisateurs se connectent à votre instance via l'adresse IP privée de l'instance, vous devez établir une connectivité réseau privée avec votre VPC, par exemple en utilisant ou en peering VPC AWS Direct Connect AWS Site-to-Site VPN, afin que vos utilisateurs puissent accéder à l'adresse IP privée de l'instance.

Si votre instance ne possède pas d'adresse IPv4 publique et que vous préférez ne pas configurer l'accès au réseau comme décrit ci-dessus, vous pouvez envisager le point de terminaison EC2 Instance Connect comme alternative à EC2 Instance Connect. Le point de terminaison EC2 Instance

Connect vous permet de vous connecter à une instance via SSH ou RDP sans qu'il soit nécessaire que l'instance dispose d'une adresse IPv4 publique. Pour plus d'informations, consultez [Connexion à votre instance Linux à l'aide de la console Amazon EC2](#).

Règle de groupe de sécurité

Vérifiez que le groupe de sécurité associé à votre instance [autorise le trafic SSH entrant](#) sur le port 22 à partir de votre adresse IP ou de votre réseau. Le groupe de sécurité par défaut pour le VPC n'autorise pas le trafic SSH entrant par défaut. Le groupe de sécurité créé par l'assistant de lancement de l'instance autorise par défaut le trafic SSH entrant. Pour plus d'informations, consultez [Règles pour la connexion à des instances à partir de votre ordinateur](#).

EC2 Instance Connect utilise des plages d'adresses IP spécifiques pour les connexions SSH par navigateur à votre instance (lorsque les utilisateurs utilisent la console Amazon EC2 pour se connecter à une instance). Si vos utilisateurs utiliseront la console Amazon EC2 pour se connecter à une instance, assurez-vous que le groupe de sécurité associé à votre instance autorise le trafic SSH entrant à partir de la plage d'adresses IP pour EC2_INSTANCE_CONNECT. Pour identifier la plage d'adresses, téléchargez le fichier JSON fourni par AWS et filtrez le sous-ensemble pour EC2 Instance Connect, en utilisant EC2_INSTANCE_CONNECT comme valeur de service. Ces plages d'adresses IP diffèrent entre les deux Régions AWS. Pour plus d'informations sur le téléchargement du fichier JSON et le filtrage par service, consultez [Plages d'adresses IP AWS](#) dans le Guide de l'utilisateur Amazon VPC.

Accorder des autorisations

Vous devez accorder les autorisations requises à chaque utilisateur IAM qui utilisera EC2 Instance Connect pour se connecter à une instance. Pour plus d'informations, consultez [Accorder des autorisations IAM pour EC2 Instance Connect](#).

Configuration de l'ordinateur local

Si vos utilisateurs se connectent en utilisant SSH, ils doivent s'assurer que leur ordinateur local dispose d'un client SSH.

L'ordinateur local d'un utilisateur dispose probablement d'un client SSH installé par défaut. Il peut vérifier la présence d'un client SSH en saisissant ssh sur la ligne de commande. Si l'ordinateur local ne reconnaît pas la commande, l'utilisateur peut installer un client SSH. Pour plus d'informations sur l'installation d'un client SSH sur Linux ou macOS X, consultez <http://www.openssh.com>. Pour plus d'informations sur l'installation d'un client SSH sous Windows 10, consultez [OpenSSH dans Windows](#).

Il n'est pas nécessaire d'installer un client SSH sur un ordinateur local si vos utilisateurs n'utilisent que la console Amazon EC2 pour se connecter à une instance.

Nom d'utilisateur

Lorsque vous utilisez EC2 Instance Connect pour vous connecter à une instance, le nom d'utilisateur doit répondre aux conditions préalables suivantes :

- Premier caractère : doit être une lettre (A-Z, a-z), un chiffre (0-9) ou un trait de soulignement (_)
- Caractères suivants : il peut s'agir de lettres (A-Z, a-z), de chiffres (0-9) ou des caractères suivants : @ . _ -
- Longueur minimale : 1 caractère
- Longueur maximale : 31 caractères

Accorder des autorisations IAM pour EC2 Instance Connect

Pour vous connecter à une instance à l'aide d'EC2 Instance Connect, vous devez créer une politique IAM qui accorde à vos utilisateurs des autorisations pour les actions et la condition suivantes :

- Action `ec2-instance-connect:SendSSHPublicKey` – Accorde l'autorisation d'envoyer la clé publique en mode push à une instance.
- Condition `ec2:osuser` – Spécifie le nom de l'utilisateur du système d'exploitation qui peut envoyer la clé publique en mode push à une instance. Utilisez le nom d'utilisateur par défaut pour l'AMI que vous avez utilisée pour lancer l'instance. Le nom d'utilisateur par défaut pour AL2023 et Amazon Linux 2 est `ec2-user`, et pour Ubuntu, c'est `ubuntu` est le cas.
- Action `ec2:DescribeInstances` – Requis lors de l'utilisation de la console EC2 car l'encapsuleur appelle cette action. Les utilisateurs peuvent déjà disposer de l'autorisation d'appeler cette action à partir d'une autre politique.

Envisagez de limiter l'accès à des instances EC2 spécifiques. Sinon, tous les principaux IAM disposant d'une autorisation pour l'action `ec2-instance-connect:SendSSHPublicKey` peuvent se connecter à toutes les instances EC2. Vous pouvez restreindre l'accès en spécifiant des ARN de ressources ou en utilisant des balises de ressource comme [clés de condition](#).

Pour plus d'informations, consultez [Actions, ressources et clés de condition pour Amazon EC2 Instance Connect](#).

Pour obtenir des informations sur la création de politiques IAM, veuillez consulter [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM.

Autoriser les utilisateurs à se connecter à des instances spécifiques

La politique IAM suivante accorde l'autorisation de se connecter à des instances spécifiques, identifiées par leurs ARN de ressources.

Dans l'exemple de politique IAM suivant, les actions et la condition suivantes sont spécifiées :

- L'action `ec2-instance-connect:SendSSHPublicKey` accorde aux utilisateurs l'autorisation de se connecter à deux instances, spécifiées par les ARN des ressources. Pour accorder aux utilisateurs l'autorisation de se connecter à toutes les instances EC2, remplacez les ARN de ressources par le caractère générique `*`.
- La condition `ec2:osuser` accorde l'autorisation de se connecter aux instances uniquement si le nom `ami-username` est spécifié lors de la connexion.
- L'action `ec2:DescribeInstances` est spécifiée pour accorder l'autorisation aux utilisateurs qui utiliseront la console pour se connecter à vos instances. Si vos utilisateurs n'utiliseront qu'un client SSH pour se connecter à vos instances, vous pouvez omettre `ec2:DescribeInstances`. Notez que les actions `ec2:Describe*` de l'API ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, le caractère générique `*` est nécessaire dans l'élément `Resource`.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2-instance-connect:SendSSHPublicKey",
    "Resource": [
      "arn:aws:ec2:region:account-id:instance/i-1234567890abcdef0",
      "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:osuser": "ami-username"
      }
    }
  }],
  {
    "Effect": "Allow",
```

```
"Action": "ec2:DescribeInstances",
"Resource": "*"
}
]
}
```

Autoriser les utilisateurs à se connecter à des instances avec des balises spécifiques

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction de balises pouvant être associées aux utilisateurs et aux ressources. AWS Vous pouvez utiliser des balises de ressources pour contrôler l'accès à une instance. Pour plus d'informations sur l'utilisation de balises pour contrôler l'accès à vos AWS ressources, consultez la section [Contrôle de l'accès aux AWS ressources](#) dans le guide de l'utilisateur IAM.

Dans l'exemple de politique IAM suivant, l'action `ec2-instance-connect:SendSSHPublicKey` accorde aux utilisateurs l'autorisation de se connecter à n'importe quelle instance (indiquée par le caractère générique `*` dans l'ARN de la ressource) à condition que l'instance dispose d'une balise de ressource avec `key=tag-key` et `value=tag-value`.

L'action `ec2:DescribeInstances` est spécifiée pour accorder l'autorisation aux utilisateurs qui utiliseront la console pour se connecter à vos instances. Si vos utilisateurs n'utiliseront qu'un client SSH pour se connecter à vos instances, vous pouvez omettre `ec2:DescribeInstances`. Notez que les actions `ec2:Describe*` de l'API ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, le caractère générique `*` est nécessaire dans l'élément `Resource`.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2-instance-connect:SendSSHPublicKey",
    "Resource": "arn:aws:ec2:region:account-id:instance/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/tag-key": "tag-value"
      }
    }
  }],
  {
    "Effect": "Allow",
    "Action": "ec2:DescribeInstances",
    "Resource": "*"
  }
}
```

```
]
}
```

Installer EC2 Instance Connect sur vos instances EC2

Pour se connecter à une instance à l'aide d'EC2 Instance Connect, l'instance doit avoir EC2 Instance Connect installé.

Les AMI suivantes sont préinstallées avec EC2 Instance Connect :

- Norme AMI AL2023
- Amazon Linux 2 2.0.20190618 ou version ultérieure
- macOS Sonoma 14.2.1 ou version ultérieure
- macOS Ventura 13.6.3 ou version ultérieure
- macOS Monterey 12.7.2 ou version ultérieure
- Ubuntu 20.04 ou version ultérieure

Si votre instance a été lancée avec l'une des AMI de la liste précédente, vous pouvez ignorer cette procédure.

Note

Si vous avez configuré les paramètres `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser` pour l'authentification SSH, l'installation d'EC2 Instance Connect ne les mettra pas à jour. En conséquence, vous ne pourrez pas utiliser EC2 Instance Connect.

Conditions préalables à l'installation d'EC2 Instance Connect

- Lancez l'instance avec l'une des AMI prises en charge suivantes :

Amazon Linux 2 avant la version 2.0.20190618

AMI minimale AL2023 ou AMI optimisée pour Amazon ECS

CentOS Stream 8 et 9

macOS Sonoma avant 14.2.1, Ventura avant 13.6.3 et Monterey avant 12.7.2

Red Hat Enterprise Linux (RHEL) 8 et 9

Ubuntu 16.04 et 18.04

Si votre instance a été lancée avec une version ultérieure d'Amazon Linux 2, de macOS Sonoma, Ventura, Monterey ou Ubuntu, elle est préinstallée avec EC2 Instance Connect et vous pouvez ignorer cette procédure.

- Vérifiez les conditions préalables générales pour EC2 Instance Connect.

Pour plus d'informations, consultez [Prérequis](#).

- Vérifiez les conditions préalables requises pour la connexion à votre instance à l'aide d'un client SSH sur votre machine locale.

Si votre machine locale exécute Linux ou macOS, veuillez consulter la rubrique [Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#). Si votre machine locale exécute Windows, veuillez consulter la rubrique [Prérequis](#).

Pour plus d'informations, consultez [Conditions préalables pour la connexion SSH](#).

- Obtenez l'ID de l'instance.

Vous pouvez obtenir l'ID de votre instance à l'aide de la console Amazon EC2 (depuis la colonne Instance ID (ID d'instance)). Si vous préférez, vous pouvez utiliser la commande [describe-instances](#) (AWS CLI) ou [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).

- Installez un client SSH sur votre ordinateur local.

Votre ordinateur local comporte probablement un client SSH par défaut. Vous pouvez vérifier un client SSH en tapant `ssh` dans la ligne de commande. Si votre ordinateur local ne reconnaît pas la commande, vous pouvez installer un client SSH. Pour plus d'informations sur l'installation d'un client SSH sur Linux ou macOS X, consultez <http://www.openssh.com>. Pour plus d'informations sur l'installation d'un client SSH sous Windows 10, consultez [OpenSSH dans Windows](#).

- (Ubuntu) Installez-le AWS CLI sur votre instance.

Pour installer EC2 Instance Connect sur une instance Ubuntu, vous devez utiliser le AWS CLI. Pour plus d'informations sur l'installation du AWS CLI, consultez la section [Installation du AWS CLI](#) dans le guide de AWS Command Line Interface l'utilisateur.

Installation d'EC2 Instance Connect

L'installation d'EC2 Instance Connect configure le démon SSH sur l'instance.

Utilisez l'une des procédures suivantes pour installer EC2 Instance Connect selon le système d'exploitation de votre instance.

Amazon Linux 2

Pour installer EC2 Instance Connect sur une instance lancée avec Amazon Linux 2

1. Connectez-vous à votre instance à l'aide de SSH.

Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de clés SSH attribuée à votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut de l'AMI que vous avez utilisée pour lancer votre instance. Pour Amazon Linux 2, le nom d'utilisateur par défaut est `ec2-user`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez [Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#).

2. Installez le package EC2 Instance Connect sur votre instance.

```
[ec2-user ~]$ sudo yum install ec2-instance-connect
```

Trois nouveaux scripts doivent apparaître dans le dossier `/opt/aws/bin/` :

```
eic_curl_authorized_keys  
eic_parse_authorized_keys  
eic_run_authorized_keys
```

3. (Facultatif) Vérifiez qu'EC2 Instance Connect a été installé avec succès sur votre instance.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config
```

EC2 Instance Connect a été correctement installé si les lignes `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser` contiennent les valeurs suivantes :

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
```

```
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` définit le script `ec2_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

Note

Si vous avez déjà configuré `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser`, l'installation d'EC2 Instance Connect ne modifie pas les valeurs et vous ne pouvez pas utiliser EC2 Instance Connect.

CentOS

Installation d'EC2 Instance Connect sur une instance lancée avec CentOS

1. Connectez-vous à votre instance à l'aide de SSH.

Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de clés SSH attribuée à votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut de l'AMI que vous avez utilisée pour lancer votre instance. Pour CentOS, le nom d'utilisateur par défaut est `centos` ou `ec2-user`.

```
$ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez [Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#).

2. Si vous utilisez un proxy HTTP ou HTTPS, vous devez définir les variables d'environnement `http_proxy` ou `https_proxy` dans la session shell en cours.

Si vous n'utilisez pas de proxy, vous pouvez ignorer cette étape.

- Pour un serveur proxy HTTP, exécutez les commandes suivantes :

```
$ export http_proxy=http://hostname:port
```

```
$ export https_proxy=http://hostname:port
```

- Pour un serveur proxy HTTPS, exécutez les commandes suivantes :

```
$ export http_proxy=https://hostname:port  
$ export https_proxy=https://hostname:port
```

3. Installez le package EC2 Instance Connect sur votre instance en exécutant les commandes suivantes.

Les fichiers de configuration EC2 Instance Connect pour CentOS sont fournis dans un package Red Hat Package Manager (RPM), avec différents packages RPM pour CentOS 8 et CentOS 9 et pour les types d'instances exécutés sur Intel/AMD (x86_64) ou ARM (AArch64).

Utilisez le bloc de commande correspondant à votre système d'exploitation et à l'architecture de votre processeur.

- CentOS 8

Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect  
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm  
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm  
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect  
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm  
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

```
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- CentOS 9

Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Vous devriez voir ce nouveau script dans le dossier `/opt/aws/bin/` :

```
eic_run_authorized_keys
```

4. (Facultatif) Vérifiez qu'EC2 Instance Connect a été installé avec succès sur votre instance.

- Pour CentOS 8 :

```
[ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

- Pour CentOS 9 :

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect a été correctement installé si les lignes `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser` contiennent les valeurs suivantes :

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` définit le script `eic_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

Note

Si vous avez déjà configuré `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser`, l'installation d'EC2 Instance Connect ne modifie pas les valeurs et vous ne pouvez pas utiliser EC2 Instance Connect.

macOS

Installation d'EC2 Instance Connect sur une instance lancée avec macOS

1. Connectez-vous à votre instance à l'aide de SSH.

Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de clés SSH attribuée à votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut de l'AMI que vous avez utilisée pour lancer votre instance. Pour les instances de macOS, le nom d'utilisateur par défaut est `ec2-user`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez [Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#).

2. Mettez à jour Homebrew en utilisant la commande suivante. La mise à jour listera les logiciels que Homebrew connaît. Le package EC2 Instance Connect est fourni via Homebrew sur les instances de macOS. Pour plus d'informations, consultez [Mettre à jour le système d'exploitation et le logiciel sur les instances Mac](#).

```
[ec2-user ~]$ brew update
```

3. Installez le package EC2 Instance Connect sur votre instance. Cela installera le logiciel et configurera sshd pour l'utiliser.

```
[ec2-user ~]$ brew install ec2-instance-connect
```

Vous devriez voir ce nouveau script dans le dossier `/opt/aws/bin/` :

```
eic_run_authorized_keys
```

4. (Facultatif) Vérifiez qu'EC2 Instance Connect a été installé avec succès sur votre instance.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect a été correctement installé si les lignes `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser` contiennent les valeurs suivantes :

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` définit le script `eic_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

Note

Si vous avez déjà configuré `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser`, l'installation d'EC2 Instance Connect ne modifie pas les valeurs et vous ne pouvez pas utiliser EC2 Instance Connect.

RHEL

Installation d'EC2 Instance Connect sur une instance lancée avec Red Hat Enterprise Linux (RHEL)

1. Connectez-vous à votre instance à l'aide de SSH.

Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de clés SSH attribuée à votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut de l'AMI que vous avez utilisée pour lancer votre instance. Pour RHEL, le nom d'utilisateur par défaut est `ec2-user` ou `root`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez [Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#).

2. Si vous utilisez un proxy HTTP ou HTTPS, vous devez définir les variables d'environnement `http_proxy` ou `https_proxy` dans la session shell en cours.

Si vous n'utilisez pas de proxy, vous pouvez ignorer cette étape.

- Pour un serveur proxy HTTP, exécutez les commandes suivantes :

```
$ export http_proxy=http://hostname:port  
$ export https_proxy=http://hostname:port
```

- Pour un serveur proxy HTTPS, exécutez les commandes suivantes :

```
$ export http_proxy=https://hostname:port
```

```
$ export https_proxy=https://hostname:port
```

3. Installez le package EC2 Instance Connect sur votre instance en exécutant les commandes suivantes.

Les fichiers de configuration EC2 Instance Connect pour RHEL sont fournis dans un package Red Hat Package Manager (RPM), avec différents packages RPM pour RHEL 8 et RHEL 9 et pour les types d'instances qui s'exécutent sur Intel/AMD (x86_64) ou ARM (AArch64).

Utilisez le bloc de commande correspondant à votre système d'exploitation et à l'architecture de votre processeur.

- RHEL 8

Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- RHEL 9

Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Vous devriez voir ce nouveau script dans le dossier `/opt/aws/bin/` :

```
eic_run_authorized_keys
```

4. (Facultatif) Vérifiez qu'EC2 Instance Connect a été installé avec succès sur votre instance.

- Pour RHEL 8 :

```
[ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-
connect.conf
```

- Pour RHEL 9 :

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect a été correctement installé si les lignes `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser` contiennent les valeurs suivantes :

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` définit le script `eic_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

Note

Si vous avez déjà configuré `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser`, l'installation d'EC2 Instance Connect ne modifie pas les valeurs et vous ne pouvez pas utiliser EC2 Instance Connect.

Ubuntu

Pour installer EC2 Instance Connect sur une instance lancée avec Ubuntu 16.04 ou version ultérieure

1. Connectez-vous à votre instance à l'aide de SSH.

Remplacez les valeurs de l'exemple dans la commande suivante par vos propres valeurs. Utilisez la paire de clés SSH attribuée à votre instance lorsque vous l'avez lancée et utilisez le nom d'utilisateur par défaut de l'AMI que vous avez utilisée pour lancer votre instance. Pour une AMI Ubuntu, le nom d'utilisateur est `ubuntu`.

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez [Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#).

- (Facultatif) Assurez-vous que votre instance possède l'AMI Ubuntu la plus récente.

Exécutez les commandes suivantes pour mettre à jour tous les paquets sur votre instance.

```
ubuntu:~$ sudo apt-get update
```

```
ubuntu:~$ sudo apt-get upgrade
```

- Installez le package EC2 Instance Connect sur votre instance.

```
ubuntu:~$ sudo apt-get install ec2-instance-connect
```

Trois nouveaux scripts doivent apparaître dans le dossier `/usr/share/ec2-instance-connect/` :

```
eic_curl_authorized_keys  
eic_parse_authorized_keys  
eic_run_authorized_keys
```

- (Facultatif) Vérifiez qu'Instance Connect a été installé avec succès sur votre instance.

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

EC2 Instance Connect a été correctement installé si les lignes `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser` contiennent les valeurs suivantes :

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %  
%u %%f  
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` définit le script `eic_run_authorized_keys` pour rechercher les clés à partir des métadonnées de l'instance.
- `AuthorizedKeysCommandUser` définit l'utilisateur système comme `ec2-instance-connect`.

Note

Si vous avez déjà configuré `AuthorizedKeysCommand` et `AuthorizedKeysCommandUser`, l'installation d'EC2 Instance Connect ne modifie pas les valeurs et vous ne pouvez pas utiliser EC2 Instance Connect.

Pour plus d'informations sur le package EC2 Instance Connect, consultez [aws/aws-ec2](#) - sur le site Web. `instance-connect-config` GitHub

Connexion à l'aide de EC2 Instance Connect

Les instructions suivantes expliquent comment vous connecter à votre instance Linux avec EC2 Instance Connect.

Décidez de l'option de connexion à utiliser. L'option de connexion à utiliser dépend du fait que votre instance dispose ou non d'une adresse IPv4 publique :

- Console Amazon EC2 – Pour se connecter à l'aide de la console Amazon EC2, l'instance doit disposer d'une adresse IPv4 publique.
- Client SSH – Si l'instance ne dispose pas d'une adresse IP publique, vous pouvez vous connecter à l'instance sur un réseau privé à l'aide d'un client SSH. Par exemple, vous pouvez vous connecter depuis le même VPC ou via une connexion VPN, transit gateway ou AWS Direct Connect.

EC2 Instance Connect ne prend pas en charge la connexion à l'aide d'une adresse IPv6.

Tip

EC2 Instance Connect est l'une des options de connexion à votre instance Linux. Pour d'autres options, veuillez consulter la rubrique [Connectez-vous à votre instance Linux](#). Pour vous connecter à une instance Windows, consultez [Connexion à votre instance Windows](#).

Options de connexion pour EC2 Instance Connect

- [Connexion à l'aide de la console Amazon EC2](#)
- [Connexion à l'aide de votre propre clé et d'un client SSH](#)

- [Connectez-vous à l'aide du AWS CLI](#)
- [Dépannage](#)

Connexion à l'aide de la console Amazon EC2

Vous pouvez vous connecter à une instance à l'aide de la console Amazon EC2 en sélectionnant l'instance à partir de la console et en choisissant de vous connecter avec EC2 Instance Connect. Instance Connect gère les autorisations et fournit une connexion réussie.

Pour se connecter à l'aide de la console Amazon EC2, l'instance doit avoir une adresse IPv4 publique. Avant de vous connecter, assurez-vous de vérifier tous les [prérequis](#).

Pour vous connecter à votre instance à l'aide du client basé sur un navigateur à partir de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance, puis choisissez Connect (Connexion).
4. Choisissez l'onglet EC2 Instance Connect.
5. Pour le type de connexion, choisissez Connect using EC2 Instance Connect.
6. Pour Nom d'utilisateur, vérifiez le nom d'utilisateur.
7. Choisissez Connecter pour ouvrir une fenêtre de terminal.

Connexion à l'aide de votre propre clé et d'un client SSH

Vous pouvez utiliser votre propre clé SSH et vous connecter à votre instance à partir du client SSH de votre choix en utilisant l'API EC2 Instance Connect. Cela vous permet de bénéficier de la capacité d'Instance Connect d'envoyer une clé publique en mode push à l'instance. Cette méthode de connexion fonctionne pour les instances avec des adresses IP publiques et privées.

Prérequis

- Exigences relatives aux paires de clés
 - Types pris en charge : RSA (OpenSSH et SSH2) et ED25519
 - Longueurs prises en charge : 2048 et 4096
 - Pour plus d'informations, consultez [Créer une paire de clés à l'aide d'un outil tiers et importer la clé publique dans Amazon EC2](#).

- Lors de la connexion à une instance qui n'a que des adresses IP privées, l'ordinateur local à partir duquel vous lancez la session SSH doit avoir une connectivité au point de terminaison du service EC2 Instance Connect (pour pousser votre clé publique SSH vers l'instance) ainsi qu'une connectivité réseau à l'adresse IP privée de l'instance pour établir la session SSH. Le point de terminaison du service EC2 Instance Connect est accessible sur Internet ou via une interface virtuelle publique AWS Direct Connect . Pour vous connecter à l'adresse IP privée de l'instance, vous pouvez tirer parti de services tels que [AWS Direct Connect](#), [AWS Site-to-Site VPN](#), ou d'un [appariage VPC](#).

Avant de vous connecter, assurez-vous de vérifier tous les [prérequis](#).

Pour vous connecter à votre instance à l'aide de votre propre clé et d'un client SSH

1. (Facultatif) Générer de nouvelles clés SSH publiques et privées

Vous pouvez générer de nouvelles clés SSH privées et publiques, `my_key` et `my_key.pub`, à l'aide de la commande suivante :

```
ssh-keygen -t rsa -f my_key
```

2. Envoyer votre clé publique SSH en mode push à l'instance

Utilisez la commande [send-ssh-public-key](#) pour pousser votre clé publique SSH vers l'instance. Si vous avez lancé votre instance à l'aide d'AL2023 ou d'Amazon Linux 2, le nom d'utilisateur par défaut pour l'AMI est `ec2-user`. Si vous avez lancé votre instance avec Ubuntu, le nom d'utilisateur par défaut pour l'AMI est `ubuntu`.

L'exemple suivant pousse la clé publique vers l'instance spécifiée dans la zone de disponibilité spécifiée, afin d'authentifier `ec2-user`.

```
aws ec2-instance-connect send-ssh-public-key \
  --region us-west-2 \
  --availability-zone us-west-2b \
  --instance-id i-001234a4bf70dec41EXAMPLE \
  --instance-os-user ec2-user \
  --ssh-public-key file://my_key.pub
```

3. Connexion à l'instance avec votre clé privée

Utilisez la commande `ssh` pour vous connecter à l'instance à l'aide de la clé privée avant que la clé publique ne soit supprimée des métadonnées de l'instance (vous disposez de 60 secondes avant qu'elle ne soit supprimée). Spécifiez la clé privée qui correspond à la clé publique, le nom d'utilisateur par défaut de l'AMI que vous avez utilisée pour lancer votre instance et le nom DNS public de l'instance (si vous vous connectez via un réseau privé, spécifiez le nom DNS privé ou l'adresse IP). Ajoutez l'option `IdentitiesOnly=yes` pour vous assurer que seuls les fichiers de la configuration `ssh` et la clé spécifiée sont utilisés pour la connexion.

```
ssh -o "IdentitiesOnly=yes" -i my_key ec2-  
user@ec2-198-51-100-1.compute-1.amazonaws.com
```

Connectez-vous à l'aide du AWS CLI

Si vous connaissez l'ID de votre instance, vous pouvez utiliser la AWS CLI commande [ec2-instance-connect pour vous connecter](#) à votre instance à l'aide d'un client SSH. Si vous ne spécifiez pas de type d'instance, EC2 Instance Connect tente automatiquement de se connecter à l'adresse IPv4 publique de votre instance. Si votre instance n'a pas d'adresse IPv4 publique, EC2 Instance Connect tente alors de se connecter à l'adresse IPv4 privée de votre instance via un [point de terminaison EC2 Instance Connect](#). Si votre instance n'a pas d'adresse IPv4 privée ou si votre VPC n'a pas de point de terminaison EC2 Instance Connect, EC2 Instance Connect essaie de se connecter à l'adresse IPv6 de votre instance.

Important

Avant de vous connecter à cette méthode, assurez-vous d'avoir configuré le AWS CLI, y compris les informations d'identification qu'il utilise, et que vous utilisez la dernière version du AWS CLI. Pour plus d'informations, consultez [Installation ou mise à jour de la dernière version de l' AWS CLI](#) (français non garanti) et [Configuration de l' AWS CLI](#) (français non garanti) dans le Guide de l'utilisateur AWS Command Line Interface .

Types de connexion

auto (default)

La CLI tente de se connecter en utilisant les adresses IP de l'instance dans l'ordre suivant et avec le type de connexion correspondant :

- IPv4 public : `direct`
- IPv4 privé : `eice`
- IPv6 : `direct`

direct

La CLI tente de se connecter en utilisant les adresses IP de l'instance dans l'ordre suivant (elle ne se connecte pas via un point de terminaison EC2 Instance Connect) :

- IPv4 public
- IPv6
- IPv4 privé

eice

La CLI utilise toujours l'adresse IPv4 privée de l'instance.

Note

Dans le futur, nous pourrions changer le comportement du type de connexion auto. Pour vous assurer que le type de connexion que vous souhaitez est utilisé, nous vous recommandons de définir explicitement `--connection-type` sur `direct` ou `eice`.

Lorsque vous vous connectez à une instance à l'aide d'EC2 Instance Connect, l'API EC2 Instance Connect envoie en mode push une clé publique SSH vers les [métadonnées de l'instance](#), où elle demeure pendant 60 secondes. La politique IAM attachée à votre utilisateur l'autorise à envoyer en mode push la clé publique vers les métadonnées de l'instance.

Pour se connecter à une instance en utilisant l'ID de l'instance

Si vous ne connaissez que l'ID de l'instance et que vous souhaitez laisser EC2 Instance Connect déterminer le type de connexion à utiliser lors de la connexion à votre instance, utilisez la commande CLI [ec2-instance-connect](#) et spécifiez `ssh` le paramètre et l'ID d'instance.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

Tip

Si un message d'erreur s'affiche lors de l'utilisation de cette commande, assurez-vous que vous utilisez AWS CLI la version 2. Le `ssh` paramètre n'est disponible que dans AWS CLI la version 2. Pour plus d'informations, consultez la section [À propos de AWS CLI la version 2](#) dans le guide de AWS Command Line Interface l'utilisateur.

Pour se connecter à une instance en utilisant l'ID de l'instance et un point de terminaison EC2 Instance Connect

Si vous voulez vous connecter à votre instance via un [point de terminaison EC2 Instance Connect](#), utilisez la commande précédente et spécifiez également le paramètre `--connection-type` avec la valeur `eice`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

Pour vous connecter à une instance en utilisant l'ID de l'instance et votre propre fichier de clé privée

Si vous voulez vous connecter à votre instance via un point de terminaison EC2 Instance Connect en utilisant votre propre clé privée, indiquez l'ID de l'instance et le chemin d'accès au fichier de clé privée. N'incluez pas `file://` dans le chemin, l'exemple suivant échouera : `file:///path/to/key`.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /  
path/to/key.pem
```

Dépannage

Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez ce qui suit.

- [Résoudre les problèmes de connexion à votre instance Linux](#)
- [Comment résoudre les problèmes de connexion à mon instance EC2 à l'aide d'Instance EC2 Connect?](#)

Désinstallation d'EC2 Instance Connect

Pour désactiver EC2 Instance Connect, connectez-vous à votre instance et désinstallez le package `ec2-instance-connect` qui est installé sur le système d'exploitation. Si la configuration `sshd` correspond à ce qui a été défini quand vous avez installé EC2 Instance Connect, la désinstallation du package `ec2-instance-connect` supprime aussi la configuration `sshd`. Si vous avez modifié la configuration `sshd` après l'installation d'EC2 Instance Connect, vous devez la mettre à jour manuellement.

Amazon Linux

Vous pouvez désinstaller EC2 Instance Connect sur AL2023 et Amazon Linux 2 version 2.0.20190618 ou ultérieure, où EC2 Instance Connect est préconfiguré.

Pour désinstaller EC2 Instance Connect sur une instance lancée avec Amazon Linux 2

1. Connectez-vous à votre instance à l'aide de SSH. Spécifiez la paire de clés SSH que vous avez utilisée pour votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut pour l'AMI AL2023 ou Amazon Linux 2, qui est `ec2-user`

Par exemple, la commande `ssh` suivante vous connecte à l'instance ayant le nom DNS public `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` en utilisant la paire de clés `my_ec2_private_key.pem`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

2. Désinstallez le package `ec2-instance-connect` à l'aide de la commande `yum`.

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

Ubuntu

Pour désinstaller EC2 Instance Connect sur une instance lancée avec une AMI Ubuntu

1. Connectez-vous à votre instance à l'aide de SSH. Spécifiez la paire de clés SSH que vous avez utilisée pour votre instance lorsque vous l'avez lancée et le nom d'utilisateur par défaut pour l'AMI Ubuntu, qui est `ubuntu`.

Par exemple, la commande ssh suivante vous connecte à l'instance ayant le nom DNS public `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` en utilisant la paire de clés `my_ec2_private_key.pem`.

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

2. Désinstallez le package `ec2-instance-connect` à l'aide de la commande `apt-get`.

```
ubuntu:~$ sudo apt-get remove ec2-instance-connect
```

Connexion à votre instance Windows

Les instances Amazon EC2 créées à partir de la plupart des Amazon Machine Images (AMIs) Windows vous permettent de vous connecter à l'aide des services Bureau à distance. Les services Bureau à distance emploient le [protocole RDP \(Remote Desktop\)](#) et vous permettent de vous connecter à l'instance et de l'utiliser comme s'il s'agissait d'un ordinateur physique (ordinateur local). Il est disponible sur la plupart des éditions de Windows et disponible pour Mac OS.

La licence pour le système d'exploitation Windows Server autorise deux connexions à distance simultanées à des fins administratives. La licence pour Windows Server est incluse dans le prix de votre instance Windows. Si vous avez besoin de plus de deux connexions à distance simultanées, vous devez acheter une licence de Services de bureau à distance (RDS). Si vous tentez une troisième connexion, une erreur se produit.

Tip

Si vous devez vous connecter à votre instance afin de résoudre les problèmes de démarrage, de configuration réseau et d'autres problèmes liés aux instances créées sur le [système Nitro AWS](#), vous pouvez utiliser la [Console série EC2 pour instances Amazon EC2](#).

Table des matières

- [Connectez-vous à votre instance Windows à l'aide d'un client RDP](#)
- [Se connecter à une instance Windows à l'aide de Fleet Manager](#)
- [Configuration de vos comptes](#)

- [Transfert de fichiers vers des instances Windows](#)

Connectez-vous à votre instance Windows à l'aide d'un client RDP

La section suivante détaille les conditions préalables et le processus de connexion à votre instance à l'aide de son adresse IPv4 ou IPv6 avec un client RDP.

Prérequis

Vous devez remplir les conditions préalables suivantes pour vous connecter à votre instance Windows à l'aide d'un client RDP.

- Installez un client RDP
 - (Windows) Windows inclut un client RDP par défaut. Pour vérifier, tapez mstsc dans une fenêtre d'invite de commande. Si votre ordinateur ne reconnaît pas cette commande, consultez la [page d'accueil Microsoft Windows](#) et recherchez la page de téléchargement de l'application Bureau à distance Microsoft.
 - (macOS X) Téléchargez l'[application Microsoft Remote Desktop](#) depuis le Mac App Store.
 - (Linux) Utilisez [Remmina](#).
- Localiser la clé privée

Vous aurez besoin du chemin d'accès qualifié complet à l'emplacement sur votre ordinateur du fichier .pem pour la paire de clés que vous avez spécifiée lorsque vous avez lancé l'instance. Pour plus d'informations, consultez [the section called "Identifier la clé publique spécifiée au lancement"](#).

Si vous ne trouvez pas votre fichier de clé privée, consultez

[Lorsque vous vous connectez à une instance Windows lancée récemment, vous déchiffrez le mot de passe du compte administrateur à l'aide de la clé privée de la paire de clés que vous avez spécifiée lors du lancement de l'instance.](#)

[Si vous perdez le mot de passe administrateur et que vous n'avez plus de clé privée, vous devez réinitialiser le mot de passe ou créer une nouvelle instance. Pour plus d'informations, consultez Réinitialisation d'un mot de passe administrateur Windows perdu ou expiré. Pour connaître les étapes de réinitialisation du mot de passe à l'aide d'un document Systems Manager, consultez Réinitialiser des mots de passe et des clés SSH sur des instances EC2 dans le Guide de l'utilisateur AWS Systems Manager .](#)

- Activer le trafic RDP entrant de votre adresse IP vers votre instance

Vérifiez que le groupe de sécurité associé à votre instance autorise le trafic RDP entrant (port 3389) à partir de votre adresse IP. Le groupe de sécurité par défaut n'autorise pas le trafic RDP entrant par défaut. Pour plus d'informations, consultez [Règles pour la connexion à des instances à partir de votre ordinateur](#).

 Tip

Vous pouvez créer un point de [terminaison EC2 Instance Connect](#) pour vous connecter à votre instance Windows à l'aide du protocole RDP sans adresse IPv4 publique.

Connectez-vous à une instance Windows à l'aide du protocole RDP et de son adresse IPv4

Pour vous connecter à une instance Windows, vous devez récupérer le mot de passe administrateur initial et utiliser ce mot de passe lorsque vous vous connectez à votre instance via Remote Desktop. Il faut quelques minutes après le lancement de l'instance pour que ce mot de passe soit disponible.

Le nom d'utilisateur par défaut du compte administrateur dépend de la langue du système d'exploitation (OS) contenu dans l'AMI. Pour déterminer le nom d'utilisateur correct, identifiez la langue du système d'exploitation de votre AMI, puis choisissez le nom d'utilisateur correspondant. Par exemple, pour un système d'exploitation anglais, le nom d'utilisateur est `Administrator`, pour un système d'exploitation français, c'est le cas `Administrateur`, et pour un système d'exploitation portugais, c'est le cas `Administrador`. Si une version linguistique du système d'exploitation ne possède pas de nom d'utilisateur dans la même langue, choisissez-le `Administrator (Other)`. Pour plus d'informations, consultez la section [Noms localisés du compte administrateur sous Windows](#) sur le Microsoft TechNet Wiki.

Si vous avez joint votre instance à un domaine, vous pouvez vous connecter à votre instance à l'aide des autorisations de domaine que vous avez définies dans AWS Directory Service. Sur l'écran de connexion Bureau à distance, au lieu d'utiliser le nom de l'ordinateur local et le mot de passe généré, utilisez le nom d'utilisateur complet pour l'administrateur (par exemple, `corp.example.com\Admin`) et le mot de passe de ce compte.

Si vous recevez une erreur lors d'une tentative de connexion à votre instance, consultez [the section called "Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant"](#).

Pour vous connecter à votre instance de Windows en utilisant un client RDP

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance, puis choisissez Connecter.
4. Sur la page Connect to instance, sélectionnez l'onglet client RDP.
5. Dans Nom d'utilisateur, choisissez le nom d'utilisateur par défaut pour le compte administrateur. Le nom d'utilisateur que vous choisissez doit correspondre à la langue du système d'exploitation (OS) contenu dans l'AMI que vous avez utilisée pour lancer votre instance. S'il n'existe aucun nom d'utilisateur dans la même langue que votre système d'exploitation, choisissez Administrator (Other).
6. Choisissez Obtenir le mot de passe.
7. Sur la page Obtenir le mot de passe Windows, procédez comme suit :
 - a. Choisissez Télécharger le fichier de clé privée et accédez au fichier de clé privée (.pem) que vous avez spécifié lors du lancement de l'instance. Sélectionnez le fichier, puis choisissez Open (Ouvrir) pour copier tout le contenu du fichier dans cette page.
 - b. Choisissez Déchiffrer le mot de passe. La page Obtenir le mot de passe Windows se ferme et le mot de passe administrateur par défaut de l'instance apparaît sous Mot de passe, en remplacement du lien Obtenir le mot de passe affiché précédemment.
 - c. Copiez le mot de passe et enregistrez-le en lieu sûr. Vous en aurez besoin pour vous connecter à l'instance.
8. Sélectionnez Télécharger le fichier Bureau à distance. Lorsque vous avez terminé de télécharger le fichier, choisissez Annuler pour revenir à la page Instances. Accédez à votre répertoire de téléchargements et ouvrez le fichier RDP.
9. Vous pouvez obtenir un avertissement indiquant que l'éditeur de la connexion à distance est inconnu. Choisissez Se connecter pour vous connecter à votre instance.
10. Le compte d'administrateur est choisi par défaut. Collez le mot de passe que vous avez copié précédemment, puis cliquez sur OK.
11. En raison de la nature des certificat auto-signés, vous pouvez obtenir un avertissement indiquant que le certificat de sécurité ne peut pas être authentifié. Effectuez l'une des actions suivantes :
 - Si vous faites confiance au certificat, choisissez Oui pour vous connecter à votre instance.
 - [Windows] Avant de continuer, comparez l'empreinte numérique du certificat avec la valeur du journal système pour confirmer l'identité de l'ordinateur distant. Choisissez Afficher le

certificat, puis sélectionnez Thumbprint dans l'onglet Détails. Comparez cette valeur à celle de RDPCERTIFICATE-THUMBPRINT la section Actions, Surveillance et résolution des problèmes, Obtenir le journal du système.

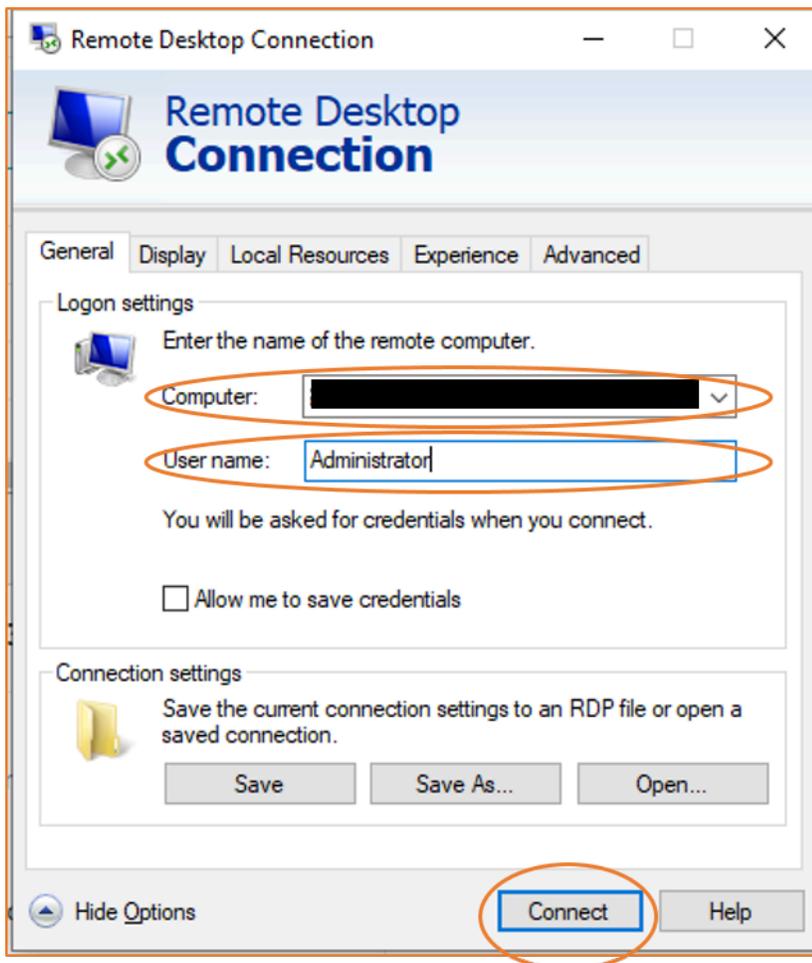
- [Mac OS X] Avant de continuer, comparez l'empreinte du certificat avec la valeur du journal système pour confirmer l'identité de l'ordinateur distant. Choisissez Afficher le certificat, développez les détails, puis choisissez SHA1 Fingerprints. Comparez cette valeur à celle de RDPCERTIFICATE-THUMBPRINT la section Actions, Surveillance et résolution des problèmes, Obtenir le journal du système.

Connectez-vous à une instance Windows à l'aide du protocole RDP et de son adresse IPv6

Si vous avez [activé votre VPC pour IPv6](#) et [attribué une adresse IPv6 à votre instance Windows](#), vous pouvez utiliser un client RDP pour vous connecter à votre instance à l'aide de son adresse IPv6 (par exemple, 2001:db8:1234:1a00:9691:9503:25ad:1761), au lieu d'une adresse IPv4 publique ou du nom d'hôte DNS public.

Pour se connecter à une instance Windows à l'aide de son adresse IPv6

1. Obtenez le mot de passe administrateur initial de votre instance, comme décrit à la section [Connectez-vous à votre instance Windows à l'aide d'un client RDP](#). Ce mot de passe est nécessaire pour établir la connexion à votre instance.
2. (Windows) Ouvrez le client RDP sur votre ordinateur Windows, choisissez Afficher les options, puis procédez comme suit :



- Pour Ordinateur, saisissez l'adresse IPv6 de votre instance Windows.
- Pour Nom d'utilisateur, entrez Administrateur.
- Choisissez Connect (Se connecter).
- Lorsque vous y êtes invité, saisissez le mot de passe que vous avez enregistré précédemment.

(macOS X) Ouvrez le client RDP sur votre ordinateur et procédez comme suit :

- Choisissez Nouveau.
- Pour Nom de l'ordinateur, saisissez l'adresse IPv6 de votre instance Windows.
- Pour Nom d'utilisateur, entrez Administrateur.
- Fermez la boîte de dialogue de Sous Mes bureaux, sélectionnez la connexion, puis Démarrer.
- Lorsque vous y êtes invité, saisissez le mot de passe que vous avez enregistré précédemment.

3. En raison de la nature des certificats auto-signés, vous pouvez obtenir un avertissement indiquant que le certificat de sécurité ne peut pas être authentifié. Si vous faites confiance au certificat, vous pouvez sélectionner Oui ou Continuer. Sinon, vous pouvez vérifier l'identité de l'ordinateur distant, comme décrit à la section [Connectez-vous à votre instance Windows à l'aide d'un client RDP](#).

Se connecter à une instance Windows à l'aide de Fleet Manager

Vous pouvez utiliser Fleet Manager, une fonctionnalité de AWS Systems Manager, pour vous connecter à des instances Windows à l'aide du protocole RDP (Remote Desktop Protocol) et afficher jusqu'à quatre instances Windows sur la même page dans le AWS Management Console. Vous pouvez vous connecter à la première instance dans le bureau à distance de Fleet Manager directement à partir de la page Instances de la console Amazon EC2. Pour plus d'informations sur Fleet Manager, consultez la section [Connexion à un nœud géré à l'aide de Remote Desktop](#) dans le Guide de l'utilisateur AWS Systems Manager .

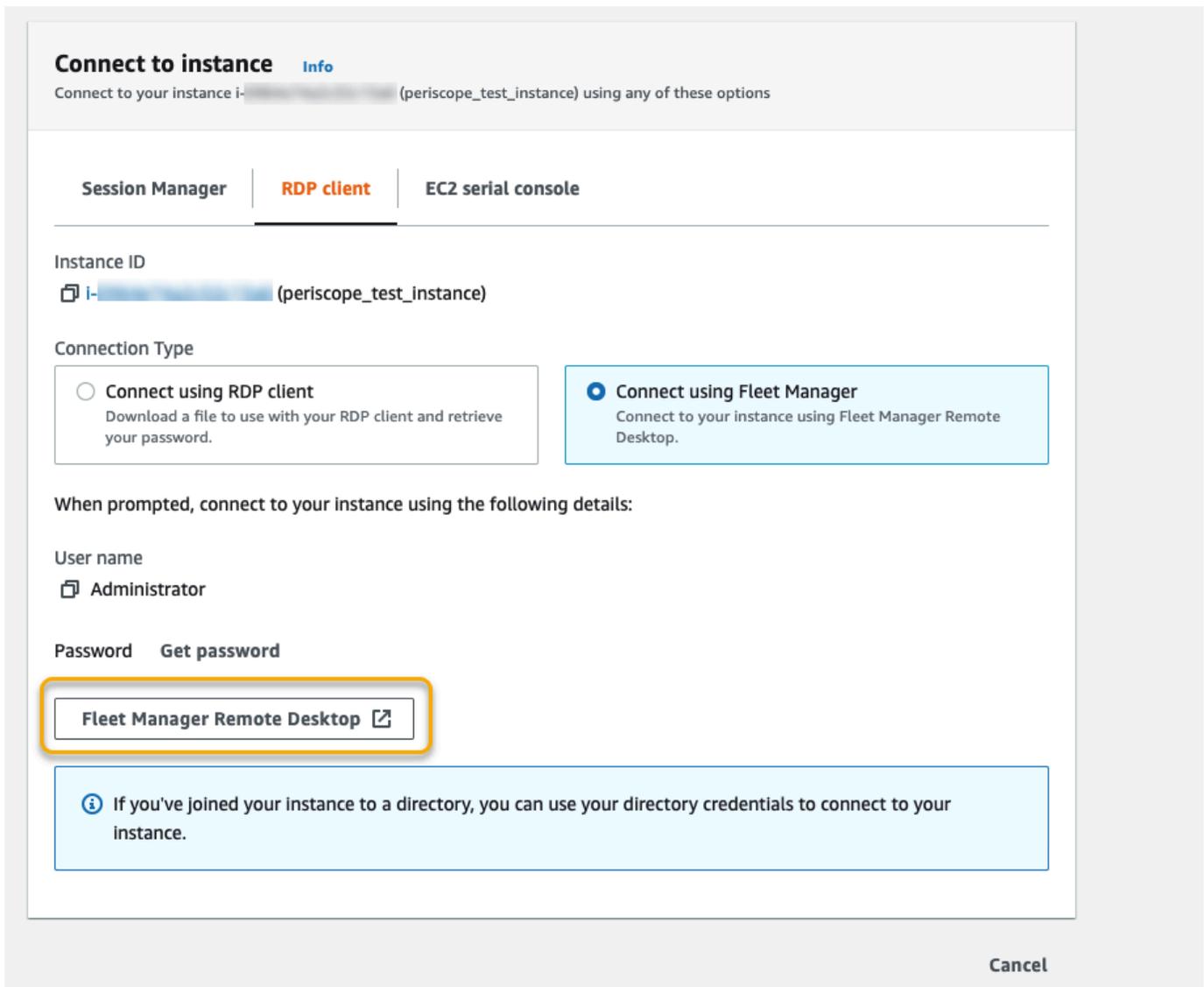
Avant d'essayer de vous connecter à une instance à l'aide de Fleet Manager, assurez-vous que les étapes d'installation nécessaires sont terminées. Pour plus d'informations, consultez [Configuration de Fleet Manager](#).

Note

Il n'est pas nécessaire d'autoriser spécifiquement le trafic RDP entrant depuis votre adresse IP si vous utilisez Fleet Manager pour vous connecter. Fleet Manager s'en charge pour vous.

Pour se connecter à des instances via RDP avec Fleet Manager (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation de gauche, choisissez Instances.
3. Sélectionnez l'instance, puis choisissez Connecter.
4. Sur la page Connect to instance (Se connecter à l'instance), choisissez l'option pour Connect using Fleet Manager (Se connecter à l'aide de Fleet Manager), puis choisissez Fleet Manager Remote Desktop (Bureau à distance Fleet Manager). Cela ouvre la page Fleet Manager Remote Desktop (Bureau à distance Fleet Manager) dans la console AWS Systems Manager .



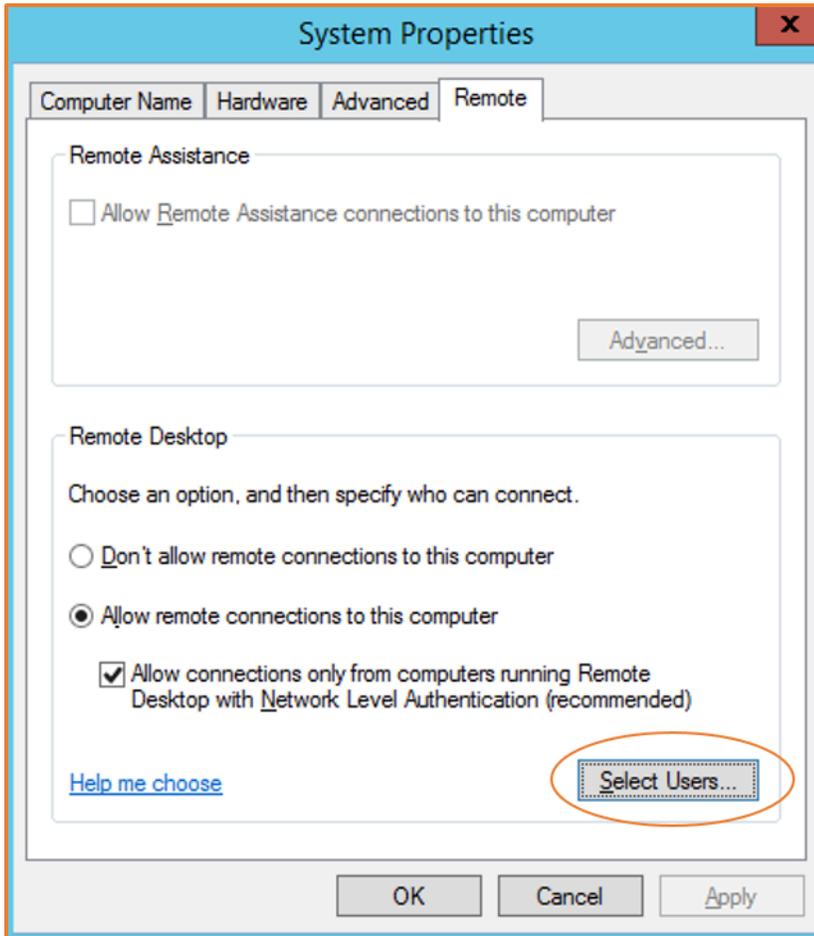
Pour plus d'informations sur la connexion à des instances Windows à partir de la page Fleet Manager Remote Desktop (Bureau à distance Fleet Manager), veuillez consulter la rubrique [Connect using Remote Desktop](#) (Se connecter l'aide du bureau à distance) dans le Guide de l'utilisateur AWS Systems Manager .

Configuration de vos comptes

Après vous être connecté via RDP, nous vous recommandons d'effectuer les opérations suivantes :

- Modifiez la valeur entrée par défaut pour le mot de passe administrateur. Il vous suffit de [modifier le mot de passe lorsque vous êtes connecté à l'instance elle-même](#), comme avec n'importe quel autre Windows Server s'exécutant sur votre ordinateur.

- Créez un autre utilisateur avec des privilèges d'administrateur sur l'instance. Il s'agit d'une protection si vous oubliez le mot de passe administrateur ou si vous rencontrez un problème avec le compte administrateur. Le nouvel utilisateur doit avoir l'autorisation d'accéder à l'instance à distance. Ouvrez Propriétés en faisant un clic droit sur l'icône Ce PC dans votre bureau Windows ou en ouvrant l'explorateur de fichiers et en sélectionnant Propriétés. Choisissez Paramètres d'utilisation à distance, puis Sélectionnez des utilisateurs pour ajouter l'utilisateur au groupe Remote Desktop Users (Utilisateurs du bureau à distance).



Transfert de fichiers vers des instances Windows

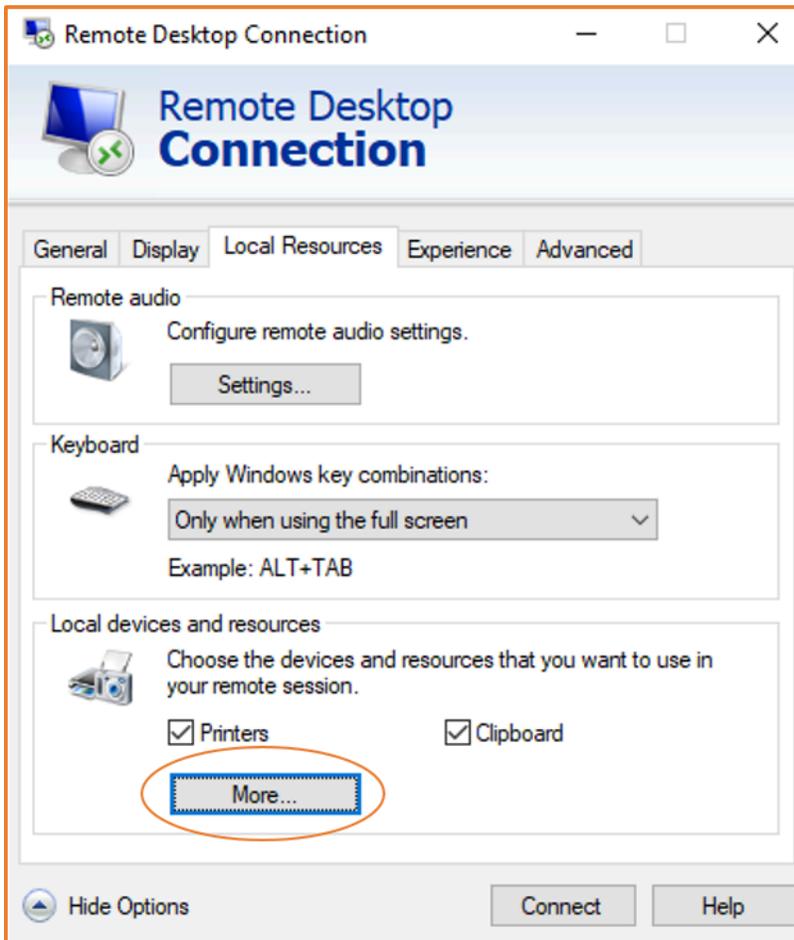
Votre instance Windows vous permet d'effectuer les mêmes opérations que n'importe quel serveur Windows. Par exemple, vous pouvez transférer des fichiers entre une instance Windows et votre ordinateur local à l'aide de la fonctionnalité de partage de fichiers local du logiciel Microsoft Remote Desktop Connection (RDP). Vous pouvez accéder aux fichiers locaux sur des disques durs, des lecteurs DVD, des lecteurs multimédia portables et des lecteurs réseau mappés.

Pour accéder à vos fichiers locaux à partir de vos instances Windows, vous devez activer la fonction de partage de fichiers locaux en mappant le lecteur de session à distance à votre lecteur local. Les étapes sont légèrement différentes selon que le système d'exploitation de votre ordinateur local est Windows ou macOS X.

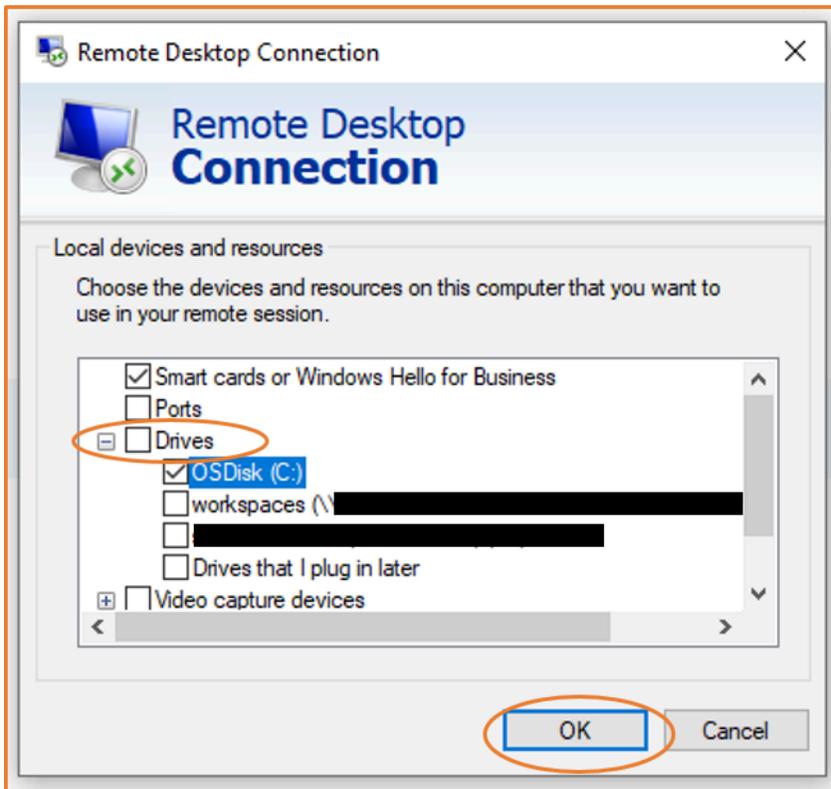
Windows

Pour mapper le lecteur de session à distance à votre lecteur local sur votre ordinateur Windows local

1. Ouvrez le client Connexion Bureau à distance.
2. Choisissez Show Options.
3. Ajoutez le nom d'hôte de l'instance au champ Computer (Ordinateur) et le nom d'utilisateur au champ User name (Nom d'utilisateur), comme suit :
 - a. Sous Connection settings (Paramètres de connexion), choisissez Open... (Ouvrir...), et accédez au fichier de raccourcis RDP que vous avez téléchargé à partir de la console Amazon EC2. Le fichier contient le nom d'hôte DNS IPv4 public, qui identifie l'instance, et le nom d'utilisateur administrateur.
 - b. Sélectionnez le fichier, puis choisissez Open (Ouvrir). Les champs Computer (Ordinateur) et User name (Nom d'utilisateur) sont remplis avec les valeurs du fichier de raccourcis RDP.
 - c. Choisissez Enregistrer.
4. Sélectionnez l'onglet Local Resources (Ressources locales).
5. Sous Local Devices and resources (Périphériques et ressources locaux), choisissez More... (Plus...).



6. Développez Lecteurs et sélectionnez le lecteur local auquel mapper l'instance Windows.
7. Choisissez OK.

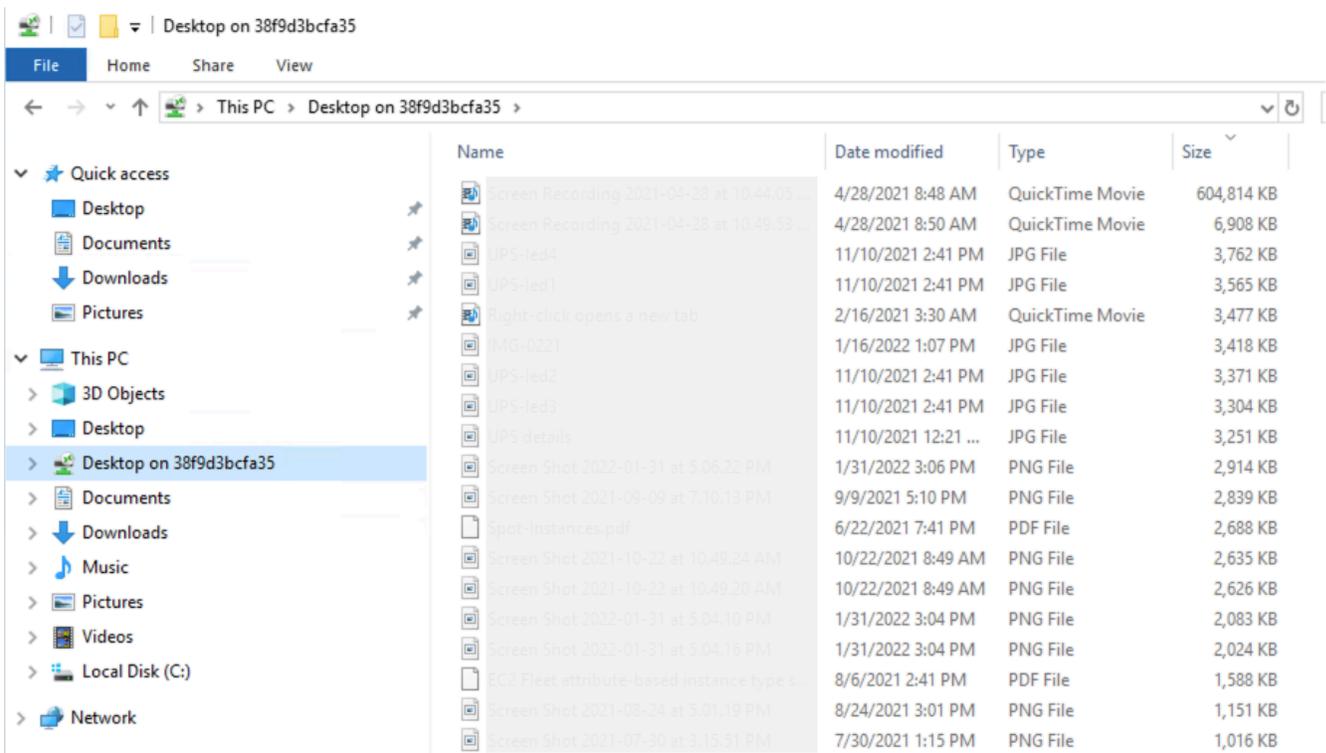


8. Choisissez Connect (Connexion) pour établir la connexion à votre instance Windows.

macOS X

Pour mapper le lecteur de session à distance à votre dossier local sur votre ordinateur macOS X local

1. Ouvrez le client Connexion Bureau à distance.
2. Accédez au fichier RDP que vous avez téléchargé depuis la console Amazon EC2 (lorsque vous vous êtes initialement connecté à l'instance) et faites-le glisser sur le client de connexion Bureau à distance.
3. Faites un clic droit sur le fichier RDP, puis choisissez Edit (Modifier).
4. Cliquez sur l'onglet Folders (Dossiers), puis cochez la case Redirect folders (Rediriger les dossiers).



Pour plus d'informations sur la mise à disposition de périphériques locaux pour une session à distance sur un ordinateur Mac, consultez [Bien démarrer avec le client macOS](#).

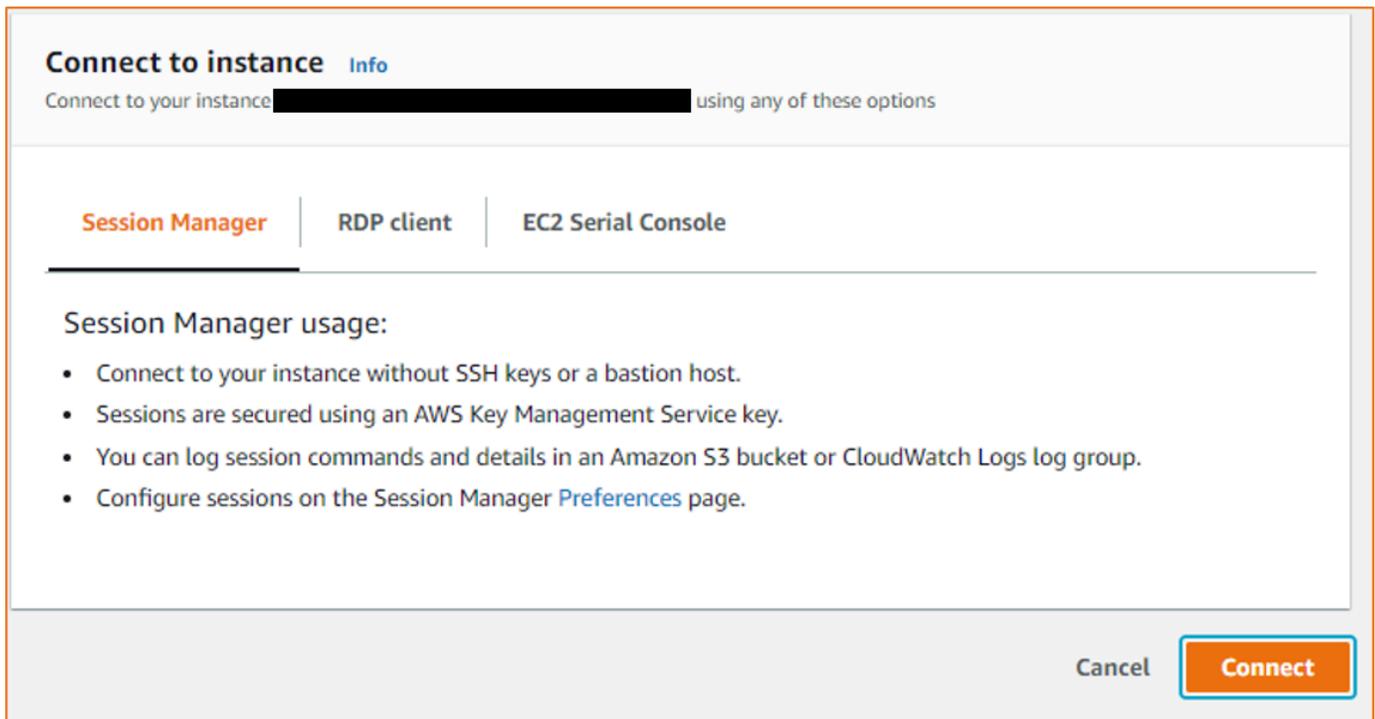
Connexion à l'aide du Gestionnaire de session

Le gestionnaire de session est une AWS Systems Manager fonctionnalité entièrement gérée permettant de gérer vos instances Amazon EC2 via un shell interactif basé sur un navigateur en un clic, ou via le AWS CLI. Vous pouvez utiliser le Gestionnaire de session pour démarrer une session avec une instance dans votre compte. Une fois la session démarrée, vous pouvez exécuter des commandes interactives sur l'instance comme vous le feriez pour tout autre type de connexion. Pour plus d'informations sur le Gestionnaire de session, consultez [Gestionnaire de sessions AWS Systems Manager](#) dans le Guide de l'utilisateur AWS Systems Manager .

Avant d'essayer de vous connecter à une instance à l'aide du Gestionnaire de session, assurez-vous que les étapes d'installation nécessaires sont terminées. Pour plus d'informations, consultez [Configuration de Session Manager](#).

Pour vous connecter à une instance Amazon EC2 à l'aide du gestionnaire de session sur la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance, puis choisissez Connect (Connexion).
4. Pour Connection method (Méthode de connexion), choisissez Session Manager (Gestionnaire de session).
5. Choisissez Connect (Se connecter).



i Tip

Si vous recevez une erreur indiquant que vous n'êtes pas autorisé à effectuer une ou plusieurs actions Systems Manager (`ssm:command-name`), vous devez mettre à jour vos stratégies qui vous permettront de démarrer des sessions à partir de la console Amazon EC2. Pour plus d'informations et d'instructions, consultez [Démarrage rapide - Politiques IAM par défaut pour Session Manager](#) dans le Guide de l'utilisateur AWS Systems Manager .

Connectez-vous à vos instances à l'aide du point de terminaison EC2 Instance Connect

Le point de terminaison EC2 Instance Connect vous permet de vous connecter en toute sécurité à une instance depuis Internet, sans utiliser d'hôte bastion ni exiger que votre cloud privé virtuel (VPC) dispose d'une connexion Internet directe.

Avantages

- Vous pouvez vous connecter à vos instances sans que celles-ci aient besoin d'une adresse IPv4 publique. AWS frais pour toutes les adresses IPv4 publiques, y compris les adresses IPv4 publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet Adresse IPv4 publique de la [page de tarification d'Amazon VPC](#).
- Vous pouvez vous connecter à vos instances depuis Internet sans que votre VPC dispose d'une connexion Internet directe via une passerelle [Internet](#).
- Vous pouvez contrôler l'accès à la création et à l'utilisation des points de terminaison EC2 Instance Connect pour vous connecter aux instances à l'aide des [politiques et autorisations IAM](#).
- Toutes les tentatives de connexion à vos instances, qu'elles soient réussies ou non, sont enregistrées [CloudTrail](#).

Tarifification

L'utilisation des points de terminaison EC2 Instance Connect est gratuite. Si vous utilisez un point de terminaison EC2 Instance Connect pour vous connecter à une instance située dans une autre zone de disponibilité, des [frais supplémentaires sont facturés pour le transfert de données](#) entre les zones de disponibilité.

Table des matières

- [Comment ça marche](#)
- [Considérations](#)
- [Accorder des autorisations pour utiliser le point de terminaison EC2 Instance Connect](#)
- [Groupes de sécurité pour le point de terminaison EC2 Instance Connect](#)
- [Création d'un point de terminaison EC2 Instance Connect](#)
- [Connectez-vous à une instance Amazon EC2 à l'aide du point de terminaison EC2 Instance Connect](#)

- [Journalisation des connexions établies via le point de terminaison EC2 Instance Connect](#)
- [Supprimer un point de terminaison EC2 Instance Connect](#)
- [Rôle lié à un service pour le point de terminaison EC2 Instance Connect](#)
- [Quotas pour le point de terminaison EC2 Instance Connect](#)

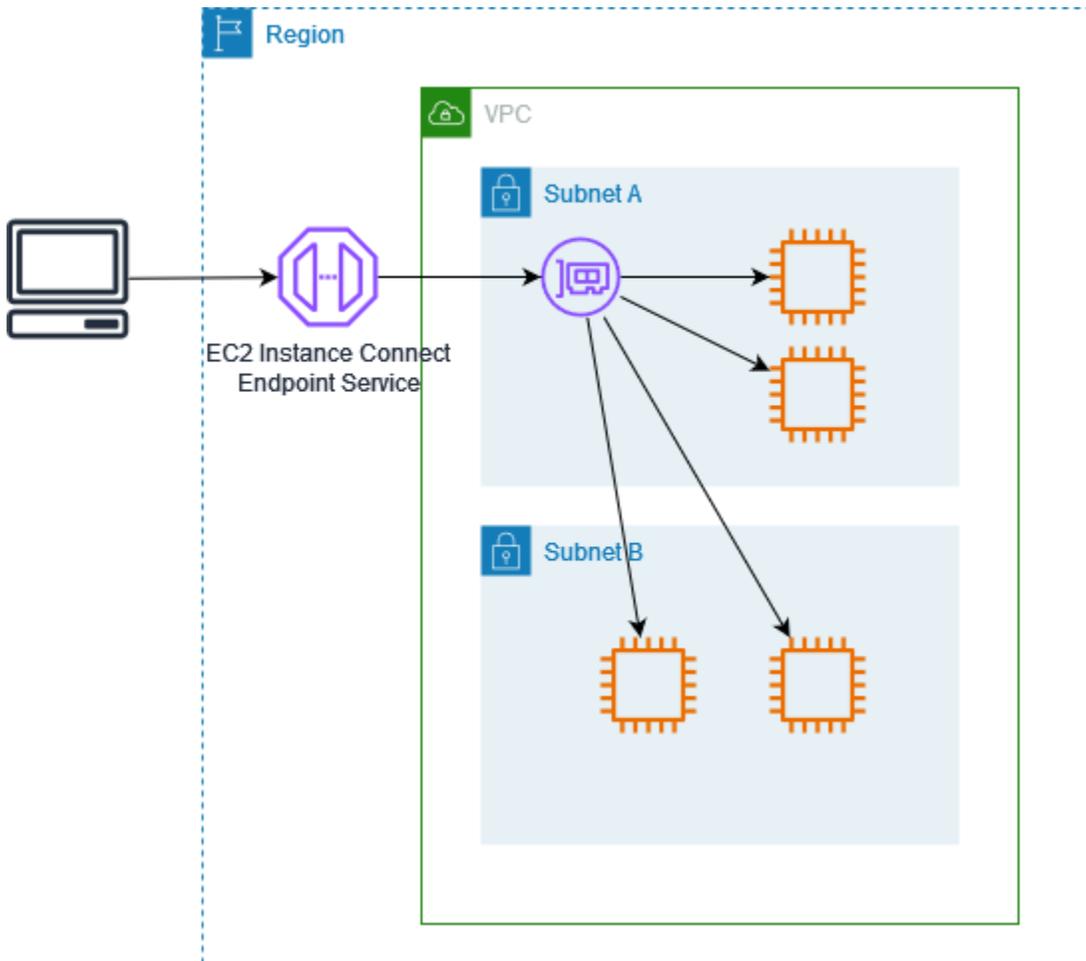
Comment ça marche

Le point de terminaison EC2 Instance Connect est un proxy TCP sensible à l'identité. Le service EC2 Instance Connect Endpoint établit un tunnel privé entre votre ordinateur et le point de terminaison à l'aide des informations d'identification de votre entité IAM. Le trafic est authentifié et autorisé avant d'atteindre votre VPC.

Vous pouvez [configurer des règles de groupe de sécurité supplémentaires](#) pour limiter le trafic entrant vers vos instances. Par exemple, vous pouvez utiliser des règles entrantes pour autoriser le trafic sur les ports de gestion uniquement à partir du point de terminaison EC2 Instance Connect.

Vous pouvez configurer les règles de table de routage pour permettre au point de terminaison de se connecter à n'importe quelle instance de n'importe quel sous-réseau du VPC.

Le schéma suivant montre comment un utilisateur peut se connecter à ses instances depuis Internet à l'aide d'un point de terminaison EC2 Instance Connect. Créez d'abord un point de terminaison EC2 Instance Connect dans le sous-réseau A. Nous créons une interface réseau pour le point de terminaison du sous-réseau, qui sert de point d'entrée pour le trafic destiné à vos instances dans le VPC. Si la table de routage du sous-réseau B autorise le trafic en provenance du sous-réseau A, vous pouvez utiliser le point de terminaison pour atteindre les instances du sous-réseau B.



Considérations

Avant de commencer, considérez les points suivants.

- Le point de terminaison EC2 Instance Connect est spécifiquement conçu pour les cas d'utilisation du trafic de gestion, et non pour les transferts de données à volume élevé. Les transferts de données à haut volume sont limités.
- Votre instance doit avoir une adresse IPv4 (privée ou publique). Le point de terminaison EC2 Instance Connect ne prend pas en charge la connexion aux instances à l'aide d'adresses IPv6.
- (Instances Linux) Si vous utilisez votre propre paire de clés, vous pouvez utiliser n'importe quelle AMI Linux. Dans le cas contraire, EC2 Instance Connect doit être installé sur votre instance. Pour plus d'informations sur les AMI qui incluent EC2 Instance Connect et sur la manière de l'installer sur d'autres AMI prises en charge, consultez [Installation d'EC2 Instance Connect](#).
- Vous pouvez attribuer un groupe de sécurité à un point de terminaison EC2 Instance Connect lorsque vous le créez. Dans le cas contraire, nous utilisons le groupe de sécurité par défaut pour le

VPC. Le groupe de sécurité d'un point de terminaison EC2 Instance Connect doit autoriser le trafic sortant vers les instances de destination. Pour plus d'informations, consultez [Groupes de sécurité pour le point de terminaison EC2 Instance Connect](#).

- Vous pouvez configurer un point de terminaison EC2 Instance Connect pour conserver les adresses IP sources des clients lors du routage des demandes vers les instances. Dans le cas contraire, l'adresse IP de l'interface réseau devient l'adresse IP du client pour tout le trafic entrant.
 - Si vous activez la préservation de l'adresse IP des clients, les groupes de sécurité des instances doivent autoriser le trafic provenant des clients. Les instances doivent également se trouver dans le même VPC que le point de terminaison EC2 Instance Connect.
 - Si vous désactivez la préservation de l'adresse IP du client, les groupes de sécurité des instances doivent autoriser le trafic en provenance du VPC. Il s'agit de l'option par défaut.
 - Les types d'instance suivants ne prennent pas en charge la préservation de l'adresse IP du client : C1, CG1, CG2, G1, H1, M1, M2, M3 et T1. Si vous activez la préservation de l'adresse IP du client et que vous tentez de vous connecter à une instance avec l'un de ces types d'instance à l'aide du point de terminaison EC2 Instance Connect, la connexion échoue.
 - La préservation de l'adresse IP du client n'est pas prise en charge lorsque le trafic est acheminé via une passerelle de transit.
- Lorsque vous créez un point de terminaison EC2 Instance Connect, un rôle lié à un service est automatiquement créé pour le service Amazon EC2 dans (IAM). AWS Identity and Access Management Amazon EC2 utilise le rôle lié à un service pour allouer des interfaces réseau dans votre compte, qui sont nécessaires lors de la création de points de terminaison EC2 Instance Connect. Pour plus d'informations, consultez [Rôle lié à un service pour le point de terminaison EC2 Instance Connect](#).
- Chaque point de terminaison EC2 Instance Connect peut prendre en charge jusqu'à 20 connexions simultanées.
- La durée maximale d'une connexion TCP établie est de 1 heure (3 600 secondes). Vous pouvez spécifier la durée maximale autorisée dans une politique IAM, qui peut aller jusqu'à 3 600 secondes. Pour plus d'informations, consultez [Autorisations permettant d'utiliser le point de terminaison EC2 Instance Connect pour se connecter aux instances](#).
- Le point de terminaison EC2 Instance Connect n'est pas pris en charge dans l'ouest du Canada (Calgary).

Accorder des autorisations pour utiliser le point de terminaison EC2 Instance Connect

Par défaut, les entités IAM ne sont pas autorisées à créer, décrire ou modifier les points de terminaison EC2 Instance Connect. Un administrateur IAM peut créer des politiques IAM qui accordent les autorisations nécessaires pour effectuer des actions spécifiques sur les ressources dont il a besoin.

Pour obtenir des informations sur la création de politiques IAM, veuillez consulter [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM.

Les exemples de politiques suivants montrent que vous pouvez contrôler les autorisations dont disposent les utilisateurs sur les points de terminaison EC2 Instance Connect.

Exemples

- [Autorisations pour créer, décrire et supprimer des points de terminaison EC2 Instance Connect](#)
- [Autorisations permettant d'utiliser le point de terminaison EC2 Instance Connect pour se connecter aux instances](#)
- [Autorisations de connexion uniquement à partir d'une plage d'adresses IP spécifique](#)

Autorisations pour créer, décrire et supprimer des points de terminaison EC2 Instance Connect

Pour créer un point de terminaison EC2 Instance Connect, les utilisateurs ont besoin d'autorisations pour les actions suivantes :

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `iam:CreateServiceLinkedRole`

Pour décrire et supprimer des points de terminaison EC2 Instance Connect, les utilisateurs ont besoin d'autorisations pour les actions suivantes :

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2>DeleteInstanceConnectEndpoint`

Vous pouvez créer une politique qui accorde l'autorisation de créer, décrire et supprimer des points de terminaison EC2 Instance Connect dans tous les sous-réseaux. Vous pouvez également

limiter les actions à des sous-réseaux spécifiques en spécifiant les ARN des sous-réseaux comme `Resource` autorisée ou en utilisant la clé de condition `ec2:SubnetID`. Vous pouvez également utiliser la clé de condition `aws:ResourceTag` pour autoriser ou refuser explicitement la création de points de terminaison avec certaines balises. Pour de plus amples informations, veuillez consulter [Politiques and permissions in IAM \(Stratégies et autorisations dans IAM\)](#) dans le IAM Guide de l'utilisateur.

Exemple de politique IAM

Dans l'exemple de politique IAM suivant, la section `Resource` accorde l'autorisation de créer et de supprimer des points de terminaison dans tous les sous-réseaux, spécifiés par l'astérisque (*). Les actions d'API `ec2:Describe*` ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, le caractère générique * est nécessaire dans l'élément `Resource`.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "GrantAllActionsInAllSubnets",
    "Action": [
      "ec2:CreateInstanceConnectEndpoint",
      "ec2>DeleteInstanceConnectEndpoint",
      "ec2:CreateNetworkInterface",
      "ec2:CreateTags",
      "iam:CreateServiceLinkedRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:subnet/*"
  },
  {
    "Action": [
      "ec2:CreateNetworkInterface"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:::security-group/*"
  },
  {
    "Sid": "DescribeInstanceConnectEndpoints",
    "Action": [
      "ec2:DescribeInstanceConnectEndpoints"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
```

```
    }  
  ]  
}
```

Autorisations permettant d'utiliser le point de terminaison EC2 Instance Connect pour se connecter aux instances

L'action `ec2-instance-connect:OpenTunnel` accorde l'autorisation d'établir une connexion TCP à une instance pour se connecter via le point de terminaison EC2 Instance Connect. Vous pouvez spécifier le point de terminaison EC2 Instance Connect à utiliser. Alternativement, une Resource avec un astérisque (*) permet aux utilisateurs d'utiliser n'importe quel point de terminaison EC2 Instance Connect disponible. Vous pouvez également limiter l'accès aux instances en fonction de la présence ou de l'absence de balises de ressources en tant que clés de condition.

Conditions

- `ec2-instance-connect:remotePort`— Le port de l'instance qui peut être utilisé pour établir une connexion TCP. Lorsque cette clé de condition est utilisée, toute tentative de connexion à une instance sur un port autre que celui spécifié dans la politique se solde par un échec.
- `ec2-instance-connect:privateIpAddress`— Adresse IP privée de destination associée à l'instance avec laquelle vous souhaitez établir une connexion TCP. Vous pouvez spécifier une seule adresse IP, telle que `10.0.0.1/32`, ou une plage d'adresses IP via des CIDR, telle que `10.0.1.0/28`. Lorsque cette clé de condition est utilisée, toute tentative de connexion à une instance ayant une adresse IP privée différente ou en dehors de la plage d'adresses CIDR se solde par un échec.
- `ec2-instance-connect:maxTunnelDuration`— Durée maximale d'une connexion TCP établie. L'unité est la seconde et la durée va d'un minimum de 1 seconde à un maximum de 3 600 secondes (1 heure). Si la condition n'est pas spécifiée, la durée par défaut est fixée à 3 600 secondes (1 heure). La tentative de connexion à une instance pendant une durée supérieure à celle spécifiée dans la politique IAM ou supérieure à la durée maximale par défaut entraîne un échec. La connexion est interrompue après la durée spécifiée.

Si `maxTunnelDuration` est spécifié dans la politique IAM et que la valeur spécifiée est inférieure à 3 600 secondes (valeur par défaut), vous devez spécifier `--max-tunnel-duration` dans la commande lors de la connexion à une instance. Pour plus d'informations sur la manière de se connecter à une instance, consultez [Connectez-vous à une instance Amazon EC2 à l'aide du point de terminaison EC2 Instance Connect](#).

Vous pouvez également accorder à un utilisateur l'accès pour établir des connexions aux instances en fonction de la présence de balises de ressources sur le point de terminaison EC2 Instance Connect. Pour de plus amples informations, veuillez consulter [Politiques and permissions in IAM \(Stratégies et autorisations dans IAM\)](#) dans le IAM Guide de l'utilisateur.

Pour les instances Linux, `ec2-instance-connect:SendSSHPublicKey` autorise le transfert de la clé publique à une instance. La condition `ec2:osuser` spécifie le nom de l'utilisateur du système d'exploitation qui peut envoyer la clé publique en mode push à une instance. Utilisez le [nom d'utilisateur par défaut pour l'AMI](#) que vous avez utilisée pour lancer l'instance. Pour plus d'informations, consultez [Accorder des autorisations IAM pour EC2 Instance Connect](#).

Exemple de politique IAM

Les exemples de politiques IAM suivants permettent à un principal IAM de se connecter à une instance en utilisant uniquement le point de terminaison EC2 Instance Connect spécifié, identifié par l'ID de point de terminaison spécifié. `eice-123456789abcdef` La connexion n'est établie avec succès que si toutes les conditions sont remplies.

Note

Les actions d'API `ec2:Describe*` ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, le caractère générique `*` est nécessaire dans l'élément `Resource`.

Linux

Cet exemple évalue si la connexion à l'instance est établie sur le port 22 (SSH), si l'adresse IP privée de l'instance se situe dans la plage de `10.0.1.0/31` (entre `10.0.1.0` et `10.0.1.1`) et si elle `maxTunnelDuration` est inférieure ou égale à quelques secondes. `3600` La connexion est interrompue au bout de `3600` secondes (1 heure).

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "EC2InstanceConnect",
    "Action": "ec2-instance-connect:OpenTunnel",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
```

```

    "Condition": {
      "NumericEquals": {
        "ec2-instance-connect:remotePort": "22"
      },
      "IpAddress": {
        "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
      },
      "NumericLessThanEquals": {
        "ec2-instance-connect:maxTunnelDuration": "3600"
      }
    }
  },
  {
    "Sid": "SSHPublicKey",
    "Effect": "Allow",
    "Action": "ec2-instance-connect:SendSSHPublicKey",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ec2:osuser": "ami-username"
      }
    }
  },
  {
    "Sid": "Describe",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceConnectEndpoints"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
}

```

Windows

Cet exemple évalue si la connexion à l'instance est établie sur le port 3389 (RDP), si l'adresse IP privée de l'instance se situe dans la plage de 10.0.1.0/31 (entre 10.0.1.0 et 10.0.1.1) et si elle maxTunnelDuration est inférieure ou égale à quelques secondes. 3600 La connexion est interrompue au bout de 3600 secondes (1 heure).

```
{
```

```

"Version": "2012-10-17",
"Statement": [{
  "Sid": "EC2InstanceConnect",
  "Action": "ec2-instance-connect:OpenTunnel",
  "Effect": "Allow",
  "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
  "Condition": {
    "NumericEquals": {
      "ec2-instance-connect:remotePort": "3389"
    },
    "IpAddress": {
      "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
    },
    "NumericLessThanEquals": {
      "ec2-instance-connect:maxTunnelDuration": "3600"
    }
  }
},
{
  "Sid": "Describe",
  "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceConnectEndpoints"
  ],
  "Effect": "Allow",
  "Resource": "*"
}
]
}

```

Autorisations de connexion uniquement à partir d'une plage d'adresses IP spécifique

L'exemple de politique IAM suivant permet à un principal IAM de se connecter à une instance à condition qu'il se connecte à partir d'une adresse IP comprise dans la plage d'adresses IP spécifiée dans la politique. Si le principal IAM appelle `OpenTunnel` depuis une adresse IP qui n'est pas comprise dans la plage d'adresses IP `192.0.2.0/24` (exemple de plage d'adresses IP dans cette politique), la réponse est `Access Denied`. Pour de plus amples informations, veuillez consulter [aws:SourceIp](#) dans le Guide de l'utilisateur IAM.

```

{
  "Version": "2012-10-17",

```

```

"Statement": [{
  "Effect": "Allow",
  "Action": "ec2-instance-connect:OpenTunnel",
  "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
  "Condition": {
    "IpAddress": {
      "aws:SourceIp": "192.0.2.0/24"
    },
    "NumericEquals": {
      "ec2-instance-connect:remotePort": "22"
    }
  }
},
{
  "Sid": "SSHPublicKey",
  "Effect": "Allow",
  "Action": "ec2-instance-connect:SendSSHPublicKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "ec2:osuser": "ami-username"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceConnectEndpoints"
  ],
  "Resource": "*"
}
]
}

```

Groupes de sécurité pour le point de terminaison EC2 Instance Connect

Un groupe de sécurité contrôle le trafic autorisé à atteindre et à quitter les ressources auxquelles il est associé. Par exemple, nous refusons le trafic à destination et en provenance d'une instance Amazon EC2 à moins qu'il ne soit spécifiquement autorisé par les groupes de sécurité associés à l'instance.

Les exemples suivants vous montrent comment configurer les règles du groupe de sécurité pour le point de terminaison EC2 Instance Connect et les instances cibles.

Exemples

- [Règles du groupe de sécurité EC2 Instance Connect Endpoint](#)
- [Règles du groupe de sécurité de l'instance cible](#)

Règles du groupe de sécurité EC2 Instance Connect Endpoint

Les règles du groupe de sécurité pour un point de terminaison EC2 Instance Connect doivent autoriser le trafic sortant destiné aux instances cibles à quitter le point de terminaison. Vous pouvez spécifier le groupe de sécurité de l'instance ou la plage d'adresses IPv4 du VPC comme destination.

Le trafic vers le point de terminaison provient du service EC2 Instance Connect Endpoint, et il est autorisé quelles que soient les règles de trafic entrant pour le groupe de sécurité du point de terminaison. Pour contrôler qui peut utiliser le point de terminaison EC2 Instance Connect pour se connecter à une instance, utilisez une politique IAM. Pour plus d'informations, consultez [Autorisations permettant d'utiliser le point de terminaison EC2 Instance Connect pour se connecter aux instances](#).

Exemple de règle sortante : référencement de groupes de sécurité

L'exemple suivant utilise le référencement des groupes de sécurité, ce qui signifie que la destination est un groupe de sécurité associé aux instances cibles. Cette règle autorise le trafic sortant du point de terminaison vers toutes les instances qui utilisent ce groupe de sécurité.

Protocole	Destination	Plage de ports	Comment
TCP	<i>ID du groupe de sécurité de l'instance</i>	22	Autorise le trafic SSH sortant vers toutes les instances associées au groupe de sécurité d'instance

Exemple de règle sortante : plage d'adresses IPv4

L'exemple suivant autorise le trafic sortant vers la plage d'adresses IPv4 spécifiée. Les adresses IPv4 d'une instance sont attribuées à partir de son sous-réseau. Vous pouvez donc utiliser la plage d'adresses IPv4 du VPC.

Protocole	Destination	Plage de ports	Comment
TCP	<i>CIDR IPv4</i> <i>VPC</i>	22	Autorise le trafic SSH sortant vers le VPC

Règles du groupe de sécurité de l'instance cible

Les règles du groupe de sécurité pour les instances cibles doivent autoriser le trafic entrant depuis le point de terminaison EC2 Instance Connect. Vous pouvez spécifier le groupe de sécurité du point de terminaison ou une plage d'adresses IPv4 comme source. Si vous spécifiez une plage d'adresses IPv4, la source varie selon que la préservation de l'adresse IP du client est activée ou désactivée. Pour plus d'informations, consultez [Considérations](#).

Les groupes de sécurité étant dynamiques, le trafic de réponse est autorisé à quitter le VPC quelles que soient les règles de sortie applicables au groupe de sécurité d'instance.

Exemple de règle entrante : référencement de groupes de sécurité

L'exemple suivant utilise le référencement des groupes de sécurité, ce qui signifie que la source est le groupe de sécurité associé au point de terminaison. Cette règle autorise le trafic SSH entrant depuis le point de terminaison vers toutes les instances qui utilisent ce groupe de sécurité, que la préservation de l'adresse IP du client soit activée ou non. S'il n'existe aucune autre règle de groupe de sécurité entrant pour SSH, les instances acceptent le trafic SSH uniquement en provenance du point de terminaison.

Protocole	Source	Plage de ports	Comment
TCP	<i>ID du</i> <i>groupe de</i> <i>sécurité des</i> <i>terminaux</i>	22	Autorise le trafic SSH entrant depuis les ressources associées au groupe de sécurité du point de terminaison

Exemple de règle entrante : conservation de l'adresse IP du client désactivée

L'exemple suivant autorise le trafic SSH entrant à partir de la plage d'adresses IPv4 spécifiée. La préservation de l'adresse IP du client étant désactivée, l'adresse IPv4 source est l'adresse de

l'interface réseau du point de terminaison. L'adresse de l'interface réseau du point de terminaison est attribuée à partir de son sous-réseau. Vous pouvez donc utiliser la plage d'adresses IPv4 du VPC pour autoriser les connexions à toutes les instances du VPC.

Protocole	Source	Plage de ports	Comment
TCP	<i>CIDR IPv4 VPC</i>	22	Autorise le trafic SSH entrant depuis le VPC

Exemple de règle entrante : préservation de l'adresse IP du client sur

L'exemple suivant autorise le trafic SSH entrant à partir de la plage d'adresses IPv4 spécifiée. La préservation de l'adresse IP du client étant activée, l'adresse IPv4 source est l'adresse du client.

Protocole	Source	Plage de ports	Comment
TCP	<i>Plage d'adresses IPv4 publiques</i>	22	Autorise le trafic entrant depuis la plage d'adresses IPv4 du client spécifiée

Création d'un point de terminaison EC2 Instance Connect

Vous pouvez créer un point de terminaison EC2 Instance Connect pour permettre une connexion sécurisée à vos instances.

Vous ne pouvez pas modifier un point de terminaison EC2 Instance Connect une fois que vous l'avez créé. Vous devez plutôt supprimer le point de terminaison EC2 Instance Connect et en créer un nouveau avec les paramètres dont vous avez besoin.

Prérequis

Vous devez disposer des autorisations IAM requises pour créer un point de terminaison EC2 Instance Connect. Pour plus d'informations, consultez [Autorisations pour créer, décrire et supprimer des points de terminaison EC2 Instance Connect](#).

Sous-réseaux partagés

Vous pouvez créer un point de terminaison EC2 Instance Connect dans un sous-réseau partagé avec vous. Vous ne pouvez pas utiliser un point de terminaison EC2 Instance Connect créé par le propriétaire du VPC dans un sous-réseau partagé avec vous.

Créez le point de terminaison à l'aide de la console

Utilisez la procédure suivante pour créer un point de terminaison EC2 Instance Connect.

Pour créer un point de terminaison EC2 Instance Connect

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation de gauche, sélectionnez Points de terminaison.
3. Choisissez Créer un point de terminaison, puis spécifiez les paramètres du point de terminaison comme suit :
 - a. (Facultatif) Pour Balise de nom, saisissez un nom pour le point de terminaison.
 - b. Pour Catégorie de service, choisissez Point de terminaison EC2 Instance Connect.
 - c. Pour le VPC, sélectionnez le VPC qui possède les instances cibles.
 - d. (Facultatif) Pour conserver les adresses IP des clients, développez les paramètres supplémentaires et cochez la case. Sinon, l'interface réseau du point de terminaison est utilisée par défaut comme adresse IP du client.
 - e. (Facultatif) Pour Groupes de sécurité, sélectionnez le groupe de sécurité à associer au point de terminaison. Dans le cas contraire, le groupe de sécurité par défaut du VPC est utilisé par défaut. Pour plus d'informations, consultez [Groupes de sécurité pour le point de terminaison EC2 Instance Connect](#).
 - f. Pour Sous-réseau, sélectionnez le sous-réseau dans lequel créer le point de terminaison.
 - g. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
4. Vérifiez vos paramètres, puis choisissez Create endpoint.

Le statut initial du point de terminaison est En attente. Avant de pouvoir vous connecter à une instance à l'aide de ce point de terminaison, vous devez attendre que l'état du point de terminaison soit disponible. Cette opération peut prendre quelques minutes.

5. Pour vous connecter à une instance à l'aide de votre point de terminaison, consultez [Connexion à une instance](#).

Créez le point de terminaison à l'aide du AWS CLI

Utilisez la commande [create-instance-connect-endpoint](#). AWS CLI

Prérequis

Installez AWS CLI la version 2 et configurez-la à l'aide de vos informations d'identification. Pour plus d'informations, voir [Installer ou mettre à jour la dernière version du AWS CLI](#) et [Configurer le AWS CLI dans le](#) guide de AWS Command Line Interface l'utilisateur. Vous pouvez également ouvrir AWS CloudShell et exécuter AWS CLI des commandes dans son shell pré-authentifié.

Pour créer le point de terminaison

Utilisez la commande suivante pour créer une interface réseau de point de terminaison pour votre point de terminaison EC2 Instance Connect dans le sous-réseau spécifié.

```
aws ec2 create-instance-connect-endpoint --subnet-id subnet-0123456789example
```

Voici un exemple de sortie.

```
{
  "OwnerId": "111111111111",
  "InstanceConnectEndpointId": "eice-0123456789example",
  "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-connect-endpoint/eice-0123456789example",
  "State": "create-complete",
  "StateMessage": "",
  "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-endpoint.us-east-1.amazonaws.com",
  "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-endpoint.us-east-1.amazonaws.com",
  "NetworkInterfaceIds": [
    "eni-0123abcd"
  ],
  "VpcId": "vpc-0123abcd",
  "AvailabilityZone": "us-east-1a",
  "CreatedAt": "2023-04-07T15:43:53.000Z"
  "SubnetId": "subnet-0123abcd",
  "PreserveClientIp": false,
  "SecurityGroupIds": [
    "sg-0123abcd"
  ],
  "Tags": []
}
```

```
}
```

Pour surveiller le statut de création

La valeur initiale du champ `State` est `create-in-progress`. Avant de pouvoir vous connecter à une instance à l'aide de ce point de terminaison, attendez que l'état soit `create-complete`. Utilisez la [describe-instance-connect-endpoints](#) AWS CLI commande pour surveiller l'état du point de terminaison EC2 Instance Connect. Le paramètre `--query` filtre les résultats dans le `State` champ.

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-ids oice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

Voici un exemple de sortie.

```
create-complete
```

Connectez-vous à une instance Amazon EC2 à l'aide du point de terminaison EC2 Instance Connect

Vous pouvez utiliser le point de terminaison EC2 Instance Connect pour vous connecter à une instance Amazon EC2 compatible avec SSH ou RDP.

Table des matières

- [Prérequis](#)
- [Dépannage](#)

Prérequis

- Vous devez disposer des autorisations IAM requises pour vous connecter à un point de terminaison EC2 Instance Connect. Pour plus d'informations, consultez [Autorisations permettant d'utiliser le point de terminaison EC2 Instance Connect pour se connecter aux instances](#).
- Le point de terminaison EC2 Instance Connect doit être dans l'état Disponible (console) ou `create-complete` (AWS CLI). Si vous ne disposez pas d'un point de terminaison EC2 Instance Connect pour votre VPC, vous pouvez en créer un. Pour plus d'informations, consultez [Création d'un point de terminaison EC2 Instance Connect](#).
- (Instances Linux) Pour utiliser la console EC2 pour vous connecter à votre instance, ou pour utiliser la CLI pour vous connecter et demander à EC2 Instance Connect de gérer la clé éphémère,

EC2 Instance Connect doit être installé sur votre instance. Pour plus d'informations, consultez [Installation d'EC2 Instance Connect](#).

- Assurez-vous que le groupe de sécurité de l'instance autorise le trafic SSH entrant depuis le point de terminaison EC2 Instance Connect. Pour plus d'informations, consultez [Règles du groupe de sécurité de l'instance cible](#).

Connexion à votre instance Linux à l'aide de la console Amazon EC2

Vous pouvez vous connecter à une instance à l'aide de la console Amazon EC2 comme suit.

Pour vous connecter à votre instance à l'aide du client basé sur un navigateur

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance, choisissez Connect.
4. Choisissez l'onglet EC2 Instance Connect.
5. Pour Type de connexion, choisissez Connexion à l'aide du point de terminaison EC2 Instance Connect.
6. Pour le point de terminaison EC2 Instance Connect, choisissez l'ID du point de terminaison EC2 Instance Connect.
7. Pour Nom d'utilisateur, si l'AMI que vous avez utilisée pour lancer l'instance utilise un nom d'utilisateur autre que `ec2-user`, entrez le nom d'utilisateur correct.
8. Pour Durée maximale du tunnel (secondes), saisissez la durée maximale autorisée pour la connexion SSH.

La durée doit être conforme à toutes les `maxTunnelDuration` conditions spécifiées dans la politique IAM. Si vous n'avez pas accès à la politique IAM, contactez votre administrateur.

9. Choisissez Se connecter. Cela ouvre une fenêtre de terminal pour votre instance.

Se connecter à votre instance Linux à l'aide de SSH

Vous pouvez utiliser SSH pour vous connecter à votre instance Linux et utiliser la commande `open-tunnel` pour établir un tunnel privé. Vous pouvez utiliser `open-tunnel` en mode connexion unique ou multi-connexion.

Pour plus d'informations sur l'utilisation du AWS CLI pour vous connecter à votre instance via SSH, consultez [Connectez-vous à l'aide du AWS CLI](#).

Les exemples suivants utilisent [OpenSSH](#). Vous pouvez utiliser n'importe quel autre client SSH qui prend en charge le mode proxy.

Connexion simple

Pour n'autoriser qu'une seule connexion à une instance en utilisant SSH et la commande **open-tunnel**

Utilisez `ssh` et la [open-tunnel](#) AWS CLI commande comme suit. La commande proxy `-o` contient la commande `open-tunnel` qui crée le tunnel privé vers l'instance.

```
ssh -i my-key-pair.pem ec2-user@i-0123456789example \  
-o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-  
id i-0123456789example'
```

Pour :

- `-i` – Spécifie la paire de clés utilisée pour lancer l'instance.
- `ec2-user@i-0123456789example` – Spécifie le nom d'utilisateur de l'AMI qui a été utilisée pour lancer l'instance, et l'ID de l'instance.
- `--instance-id` – Spécifie l'ID de l'instance à laquelle se connecter. Vous pouvez également spécifier `%h`, qui extrait l'ID de l'instance de l'utilisateur.

Multi-connexion

Pour autoriser plusieurs connexions à une instance, exécutez d'abord la [open-tunnel](#) AWS CLI commande pour commencer à écouter les nouvelles connexions TCP, puis utilisez-la `ssh` pour créer une nouvelle connexion TCP et un tunnel privé vers votre instance.

Pour autoriser plusieurs connexions à votre instance en utilisant SSH et la commande **open-tunnel**

1. Exécutez la commande suivante pour commencer à écouter les nouvelles connexions TCP sur le port spécifié sur votre ordinateur local.

```
aws ec2-instance-connect open-tunnel \  
--instance-id i-0123456789example \  
-p 22
```

```
--local-port 8888
```

Sortie attendue

```
Listening for connections on port 8888.
```

2. Dans une nouvelle fenêtre de terminal, exécutez la commande ssh suivante pour créer une nouvelle connexion TCP et un tunnel privé vers votre instance.

```
ssh -i my-key-pair.pem ec2-user@localhost -p 8888
```

Résultat attendu : dans la première fenêtre de terminal, vous verrez ce qui suit :

```
[1] Accepted new tcp connection, opening websocket tunnel.
```

Vous pouvez également voir ce qui suit :

```
[1] Closing tcp connection.
```

Connectez-vous à votre instance Linux à l'aide du AWS CLI

Si vous ne connaissez que l'ID de votre instance, vous pouvez utiliser la AWS CLI commande [ec2-instance-connect pour vous connecter](#) à votre instance à l'aide d'un client SSH. Pour plus d'informations sur l'utilisation de la commande [ec2-instance-connect](#), consultez. [Connectez-vous à l'aide du AWS CLI](#)

Prérequis

Installez AWS CLI la version 2 et configurez-la à l'aide de vos informations d'identification. Pour plus d'informations, voir [Installer ou mettre à jour la dernière version du AWS CLI](#) et [Configurer le AWS CLI dans le](#) guide de AWS Command Line Interface l'utilisateur. Vous pouvez également ouvrir AWS CloudShell et exécuter AWS CLI des commandes dans son shell pré-authentifié.

Pour se connecter à une instance en utilisant l'ID de l'instance et un point de terminaison EC2 Instance Connect

Si vous ne connaissez que l'ID d'instance, utilisez la commande CLI [ec2-instance-connect](#) et spécifiez ssh la commande, l'ID d'instance et le paramètre avec --connection-type la valeur. eice

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

Tip

Si un message d'erreur s'affiche lors de l'utilisation de cette commande, assurez-vous que vous utilisez AWS CLI la version 2. Le `ssh` paramètre n'est disponible que dans AWS CLI la version 2. Pour plus d'informations, consultez la section [À propos de AWS CLI la version 2](#) dans le guide de AWS Command Line Interface l'utilisateur.

Connectez-vous à votre instance Windows à l'aide du point de terminaison EC2 Instance Connect

Vous pouvez utiliser le protocole de bureau à distance (RDP) sur le point de terminaison EC2 Instance Connect pour vous connecter à une instance Windows sans adresse IPv4 publique ni nom DNS public.

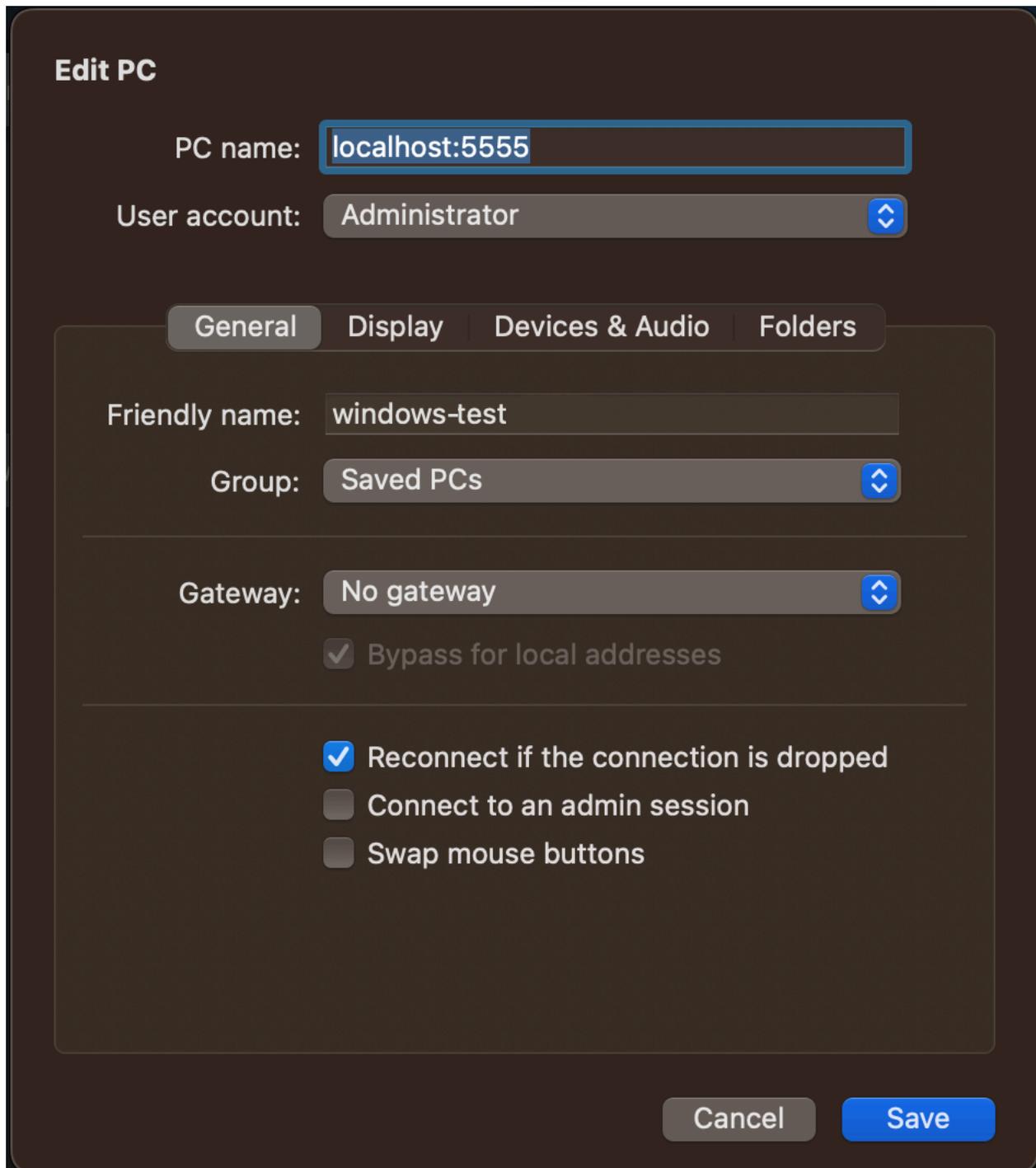
Pour vous connecter à votre instance de Windows en utilisant un client RDP

1. Effectuez les étapes 1 à 8 de la [section Connect to your Windows instance using RDP](#). Après avoir téléchargé le fichier de bureau RDP à l'étape 8, vous recevrez un message Unable to connect, ce qui est normal car votre instance ne possède pas d'adresse IP publique.
2. Exécutez la commande suivante pour établir un tunnel privé vers le VPC dans lequel se trouve l'instance. `--remote-port` doit être 3389, car le RDP utilise le port 3389 par défaut.

```
aws ec2-instance-connect open-tunnel \  
  --instance-id i-0123456789example \  
  --remote-port 3389 \  
  --local-port any-port
```

3. Dans votre dossier Téléchargements, recherchez le fichier de bureau RDP que vous avez téléchargé et faites-le glisser sur la fenêtre du client RDP.
4. Cliquez avec le bouton droit de la souris sur le fichier du bureau RDP et choisissez Modifier.
5. Dans la fenêtre Modifier le PC, pour le nom du PC (l'instance à laquelle se connecter), entrez `localhost:local-port`, where *local-port* utilise la même valeur que celle que vous avez spécifiée à l'étape 2, puis choisissez Enregistrer.

Notez que la capture d'écran suivante de la fenêtre Modifier le PC provient de Microsoft Remote Desktop sur Mac. Si vous utilisez un client Windows, la fenêtre peut être différente.



6. Dans le client RDP, faites un clic droit sur le PC (que vous venez de configurer) et choisissez Connecter pour vous connecter à votre instance.
7. À l'invite, saisissez le mot de passe déchiffré du compte administrateur.

Dépannage

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes que vous pourriez rencontrer lorsque vous utilisez le point de terminaison EC2 Instance Connect pour vous connecter à une instance.

Impossible de se connecter à votre instance

Les raisons les plus courantes pour lesquelles vous ne pouvez pas vous connecter à votre instance sont les suivantes.

- **Groupes de sécurité** : vérifiez les groupes de sécurité affectés au point de terminaison EC2 Instance Connect et à votre instance. Pour plus d'informations sur les règles de groupe de sécurité requises, consultez [Groupes de sécurité pour le point de terminaison EC2 Instance Connect](#).
- **État de l'instance** : vérifiez que l'état de votre instance est `running`.
- **Paire de clés** : si la commande que vous utilisez pour vous connecter nécessite une clé privée, vérifiez que votre instance possède une clé publique et que vous disposez de la clé privée correspondante.
- **Autorisations IAM** : vérifiez que vous disposez des autorisations IAM requises. Pour plus d'informations, consultez [Accorder des autorisations pour utiliser le point de terminaison EC2 Instance Connect](#).

Pour plus de conseils de résolution des problèmes relatifs aux instances Linux, consultez [Résoudre les problèmes de connexion à votre instance Linux](#). Pour obtenir des conseils de résolution des problèmes relatifs aux instances Windows, consultez [the section called "Connexion à votre instance Windows"](#).

ErrorCode: AccessDeniedException

Si vous recevez une erreur `AccessDeniedException` et que la condition `maxTunnelDuration` est spécifiée dans la politique IAM, veillez à spécifier le paramètre `--max-tunnel-duration` lors de la connexion à une instance. Pour plus d'informations sur ce paramètre, consultez [open-tunnel](#) dans la Référence de la commande AWS CLI .

Journalisation des connexions établies via le point de terminaison EC2 Instance Connect

Vous pouvez enregistrer les opérations sur les ressources et auditer les connexions établies via le point de terminaison EC2 Instance Connect à l'aide de AWS CloudTrail journaux.

Pour plus d'informations sur l'utilisation AWS CloudTrail avec Amazon EC2, consultez. [Enregistrez les appels d'API Amazon EC2 à l'aide de AWS CloudTrail](#)

Enregistrez les appels d'API EC2 Instance Connect Endpoint avec AWS CloudTrail

Les opérations sur les ressources du point de terminaison EC2 Instance Connect sont enregistrées en CloudTrail tant qu'événements de gestion. Lorsque les appels d'API suivants sont effectués, l'activité est enregistrée en tant qu' CloudTrail événement dans l'historique des événements :

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#) dans le Guide de AWS CloudTrail l'utilisateur.

Utilisation d' AWS CloudTrail pour auditer les utilisateurs qui se connectent à une instance à l'aide du point de terminaison EC2 Instance Connect

Les tentatives de connexion aux instances via le point de terminaison EC2 Instance Connect sont enregistrées CloudTrail dans l'historique des événements. Lorsqu'une connexion à une instance est initiée via un point de terminaison EC2 Instance Connect, la connexion est enregistrée en tant qu'événement CloudTrail de gestion avec le signe `eventName` de `OpenTunnel`.

Vous pouvez créer des EventBridge règles Amazon qui acheminent l' CloudTrail événement vers une cible. Pour plus d'informations, consultez le [guide de EventBridge l'utilisateur Amazon](#).

Voici un exemple d'événement de `OpenTunnel` gestion connecté CloudTrail.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "ABCDEFGHIJGONGNOM00CB6XYTQEXAMPLE",
    "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
    "accountId": "123456789012",
    "accessKeyId": "ABCDEFGHIJKZHN40SN2AEXAMPLE",
    "userName": "IAM-friendly-name"
  }
}
```

```
},
"eventTime": "2023-04-11T23:50:40Z",
"eventSource": "ec2-instance-connect.amazonaws.com",
"eventName": "OpenTunnel",
"awsRegion": "us-east-1",
"sourceIPAddress": "1.2.3.4",
"userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
"requestParameters": {
  "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
  "maxTunnelDuration": "3600",
  "remotePort": "22",
  "privateIpAddress": "10.0.1.1"
},
"responseElements": null,
"requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
"eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
"readOnly": false,
"resources": [{
  "accountId": "123456789012",
  "type": "AWS::EC2::InstanceConnectEndpoint",
  "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
}],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}
```

Supprimer un point de terminaison EC2 Instance Connect

Lorsque vous avez terminé d'utiliser un point de terminaison EC2 Instance Connect, vous pouvez le supprimer.

Vous devez disposer des autorisations IAM requises pour créer un point de terminaison EC2 Instance Connect. Pour plus d'informations, consultez [Autorisations pour créer, décrire et supprimer des points de terminaison EC2 Instance Connect](#).

Lorsque vous supprimez un point de terminaison EC2 Instance Connect à l'aide de la console, il passe à l'état Suppression. Si la suppression est réussie, le point de terminaison supprimé n'apparaît plus. Si la suppression échoue, l'état est rétabli `delete-failed` et le message d'état indique la raison de l'échec.

Lorsque vous supprimez un point de terminaison EC2 Instance Connect à l'aide du AWS CLI, il passe à l'état `delete-in-progress`. Si la suppression est réussie, elle passe à l'état `delete-complete`. Si la suppression échoue, l'état est rétabli `delete-failed` et `StateMessage` indique la raison de l'échec.

Console

Pour supprimer un point de terminaison EC2 Instance Connect

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation de gauche, sélectionnez Points de terminaison.
3. Sélectionnez le point de terminaison.
4. Choisissez Actions, Delete VPC endpoints (Supprimer le point de terminaison de VPC).
5. À l'invite de confirmation, saisissez **delete**.
6. Sélectionnez Delete (Supprimer).

AWS CLI

Pour supprimer un point de terminaison EC2 Instance Connect

Utilisez la [delete-instance-connect-endpoints](#) AWS CLI commande et spécifiez l'ID du point de terminaison EC2 Instance Connect à supprimer.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-id eice-03f5e49b83924bbc7
```

Exemple de sortie

```
{
  "InstanceConnectEndpoint": {
    "OwnerId": "111111111111",
    "InstanceConnectEndpointId": "eice-0123456789example",
    "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-connect-endpoint/eice-0123456789example",
    "State": "delete-in-progress",
    "StateMessage": "",
    "NetworkInterfaceIds": [],
    "VpcId": "vpc-0123abcd",
    "AvailabilityZone": "us-east-1d",
```

```
    "CreatedAt": "2023-02-07T12:05:37+00:00",  
    "SubnetId": "subnet-0123abcd"  
  }  
}
```

Rôle lié à un service pour le point de terminaison EC2 Instance Connect

[Amazon EC2 utilise des rôles liés à un AWS Identity and Access Management service \(IAM\)](#). Un rôle lié à un service est un type unique de rôle IAM qui est lié directement à Amazon EC2. Les rôles liés à un service sont prédéfinis par Amazon EC2 et incluent toutes les autorisations requises pour qu'Amazon EC2 puisse appeler d'autres personnes en votre nom. Services AWS Pour plus d'informations, consultez [Utilisation des rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Autorisations de rôle liées au service pour le point de terminaison EC2 Instance Connect

Amazon EC2 permet de créer et `AWSServiceRoleForEC2InstanceConnect` de gérer les interfaces réseau de votre compte requises par le point de terminaison EC2 Instance Connect.

Le rôle `AWSServiceRoleForEC2InstanceConnect` lié à un service fait confiance aux services suivants pour assumer le rôle :

- `ec2-instance-connect.amazonaws.com`

Le rôle `AWSServiceRoleForEC2InstanceConnect` lié au service utilise la politique gérée `InstanceConnectEc2 Endpoint`. Pour consulter les autorisations associées à cette politique, consultez [Ec2 InstanceConnect Endpoint](#) dans le manuel AWS Managed Policy Reference.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour EC2 Instance Connect Endpoint

Vous n'avez pas besoin de créer manuellement un rôle lié au service . Lorsque vous créez un point de terminaison EC2 Instance Connect, Amazon EC2 crée le rôle lié au service pour vous.

Modifier un rôle lié à un service pour EC2 Instance Connect Endpoint

Le point de terminaison EC2 Instance Connect ne vous permet pas de modifier le rôle lié au `AWSServiceRoleForEC2InstanceConnect` service.

Supprimer un rôle lié à un service pour EC2 Instance Connect Endpoint

Si vous n'avez plus besoin d'utiliser le point de terminaison EC2 Instance Connect, nous vous recommandons de supprimer le rôle lié au `AWSServiceRoleForEC2InstanceConnectservice`.

Vous devez supprimer toutes les ressources du point de terminaison EC2 Instance Connect avant de pouvoir supprimer le rôle lié à un service.

Pour supprimer le rôle lié à un service, consultez la section [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Quotas pour le point de terminaison EC2 Instance Connect

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à la région.

Vous disposez Compte AWS des quotas suivants relatifs au point de terminaison EC2 Instance Connect.

Description	Quota
Nombre maximal de points de terminaison EC2 Instance Connect par personne Compte AWS Région AWS	5
Nombre maximum de points de terminaison EC2 Instance Connect par VPC	1
Nombre maximum de points de terminaison EC2 Instance Connect par sous-réseau	1
Nombre maximal de connexions simultanées par point de terminaison EC2 Instance Connect	20

Connexion de votre instance EC2 à une ressource AWS

Après avoir lancé une instance, vous pouvez la connecter à une ou plusieurs AWS ressources.

Cette section décrit comment connecter automatiquement une instance Amazon EC2 à une base de données Amazon RDS.

Connexion automatique d'une instance EC2 à une base de données RDS

Vous pouvez utiliser la fonctionnalité de connexion automatique de la console Amazon EC2 pour connecter rapidement une ou plusieurs instances EC2 à une base de données RDS afin de permettre le trafic entre elles.

Pour plus d'informations, consultez [Mode de configuration automatique de la connexion](#). Pour une démonstration détaillée, qui inclut d'autres façons de connecter une instance EC2 et une base de données RDS, consultez [Tutoriel : Connexion d'une instance Amazon EC2 à une base de données Amazon RDS](#).

Rubriques

- [Coûts](#)
- [Prérequis](#)
- [Connexion automatique d'une instance et d'une base de données](#)
- [Mode de configuration automatique de la connexion](#)

Coûts

Bien que la connexion automatique de votre instance EC2 à une base de données RDS soit gratuite, les services sous-jacents vous sont facturés. Des frais de transfert de données s'appliquent si votre instance EC2 et votre base de données RDS se trouvent dans des zones de disponibilité différentes. Pour plus d'informations sur les frais de transfert de données, consultez [Transfert de données](#) sur la page Tarification à la demande d'Amazon EC2.

Prérequis

Avant de pouvoir connecter automatiquement une instance EC2 à une base de données RDS, vérifiez les points suivants :

- Les instances EC2 doivent être dans l'état Running (En cours d'exécution). Vous ne pouvez pas connecter une instance EC2 si elle est dans un autre état.
- Les instances EC2 et la base de données RDS doivent se trouver dans le même cloud privé virtuel (VPC). La fonction de connexion automatique n'est pas prise en charge si une instance EC2 et une base de données RDS se trouvent dans des VPC différents.

Connexion automatique d'une instance et d'une base de données

Vous pouvez connecter automatiquement une instance EC2 à une base de données RDS immédiatement après le lancement de votre instance, ou plus tard.

Connexion automatique immédiatement après le lancement

Suivez les étapes suivantes pour connecter automatiquement une instance EC2 à une base de données RDS immédiatement après avoir lancé l'instance EC2.

Pour voir une animation de ces étapes, consultez [Voir une animation : Connexion automatique d'une instance EC2 nouvellement lancée à une base de données RDS](#).

Connexion automatique d'une instance EC2 nouvellement lancée à une base de données RDS à l'aide de la console EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le tableau de bord de la console, choisissez Launch instances (Lancer des instances), puis suivez les étapes pour [lancer une instance](#).
3. Sur la page de confirmation du lancement de l'instance, choisissez Connect an RDS database (Connecter une base de données RDS).
4. Dans la boîte de dialogue Connect RDS Database (Connecter une base de données RDS), effectuez les opérations suivantes :
 - a. Pour Database role (Rôle de la base de données), sélectionnez soit Cluster soit Instance.
 - b. Pour RDS database (Base de données RDS), sélectionnez une base de données à laquelle vous connecter.

Note

Les instances EC2 et la base de données RDS doivent se trouver dans le même VPC pour pouvoir se connecter l'une à l'autre.

- c. Choisissez Se connecter.

Voir une animation : Connexion automatique d'une instance EC2 nouvellement lancée à une base de données RDS

The screenshot displays the Amazon EC2 console interface. On the left is a navigation sidebar with categories like EC2 Dashboard, Instances, Images, Elastic Block Store, and Network & Security. The main content area is divided into several panels:

- Resources:** A summary table showing EC2 resources in the Europe (Stockholm) Region:

Instances (running)	1	Dedicated Hosts	0	Elastic IPs	0
Instances	1	Key pairs	1	Load balancers	0
Placement groups	0	Security groups	9	Snapshots	1
Volumes	2				
- Launch instance:** A section with a "Launch instance" button and a "Migrate a server" link. A note states: "Your instances will launch in the Europe (Stockholm) Region".
- Scheduled events:** A section for the "Europe (Stockholm)" region showing "No scheduled events".
- Migrate a server:** A section with the text: "Use AWS Application Migration Service to simplify and expedite migration".
- Service health:** Shows the region as "Europe (Stockholm)" and the status as "This service is operating normally".
- Zones:** A table listing available zones:

Zone name	Zone ID
eu-north-1a	eun1-az1
eu-north-1b	eun1-az2
eu-north-1c	eun1-az3

On the right side, there are panels for "Account at" (showing VPC, Default VPC, etc.), "Explore AV" (Amazon GuardDuty, etc.), and "Additional" (Getting started).

Connexion automatique d'une instance existante

Suivez les étapes suivantes pour connecter automatiquement une instance EC2 existante à une base de données RDS.

Pour voir une animation de ces étapes, consultez [Voir une animation : Connexion automatique d'une instance EC2 existante à une base de données RDS](#).

Connexion automatique d'une instance EC2 existante à une base de données RDS à l'aide de la console EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez une ou plusieurs instances EC2 à connecter à une base de données RDS, puis choisissez Actions, Networking (Réseaux), Connect RDS database (Connecter la base de données RDS).

Si Connect RDS database (Connecter la base de données RDS) n'est pas disponible, vérifiez que les instances EC2 sont dans l'état Running (En cours d'exécution) et qu'elles se trouvent dans le même VPC.

4. Dans la boîte de dialogue Connect RDS Database (Connecter une base de données RDS), effectuez les opérations suivantes :
 - a. Pour Database role (Rôle de la base de données), sélectionnez soit Cluster soit Instance.
 - b. Pour RDS database (Base de données RDS), sélectionnez une base de données à laquelle vous connecter.

Note

Les instances EC2 et la base de données RDS doivent se trouver dans le même VPC pour pouvoir se connecter l'une à l'autre.

- c. Choisissez Se connecter.

Voir une animation : Connexion automatique d'une instance EC2 existante à une base de données RDS

The screenshot shows the AWS Management Console interface for the EC2 Dashboard in the Europe (Stockholm) region. The main content area is divided into several sections:

- Resources:** A table showing the number of various Amazon EC2 resources in the region.

Resource	Count
Instances (running)	2
Instances	2
Placement groups	0
Volumes	3
Dedicated Hosts	0
Key pairs	1
Security groups	10
Elastic IPs	0
Load balancers	0
Snapshots	1
- Launch instance:** A section with a "Launch Instance" button and a "Migrate a server" link. A note indicates that instances will launch in the Europe (Stockholm) Region.
- Scheduled events:** A section showing "No scheduled events" for the Europe (Stockholm) region.
- Migrate a server:** A section with a link to "Use AWS Application Migration Service to simplify and expedite migration".
- Service health:** A section showing the status of the service. The region is Europe (Stockholm) and the status is "This service is operating normally".
- Zones:** A table listing the available Availability Zones in the region.

Zone name	Zone ID
eu-north-1a	eun1-az1
eu-north-1b	eun1-az2
eu-north-1c	eun1-az3

On the right side of the dashboard, there are sections for "Account attributes" (including supported platforms, VPC, and settings) and "Explore AWS" (highlighting features like Amazon GuardDuty Malware Protection and AWS Graviton2).

Pour plus d'informations sur la façon d'utiliser la console Amazon RDS pour connecter automatiquement une instance EC2 à une base de données RDS, consultez [Configurer la connectivité réseau automatique avec une instance EC2](#) dans le Guide de l'utilisateur Amazon RDS.

Mode de configuration automatique de la connexion

Lorsque vous utilisez la console EC2 pour configurer automatiquement la connexion entre une instance EC2 et une base de données RDS afin de permettre le trafic entre elles, la connexion est configurée par des [groupes de sécurité](#).

Les groupes de sécurité sont automatiquement créés et ajoutés à l'instance EC2 et à la base de données RDS, comme suit :

- Amazon EC2 crée un groupe de sécurité appelé `ec2-rds-x` et l'ajoute à l'instance EC2. Il possède une règle sortante qui autorise le trafic vers la base de données en spécifiant `rds-ec2-x` (le groupe de sécurité de la base de données) comme destination.
- Amazon RDS crée un groupe de sécurité appelé `rds-ec2-x` et l'ajoute à la base de données. Il possède une règle entrante qui autorise le trafic provenant de l'instance EC2 en spécifiant `ec2-rds-x` (le groupe de sécurité de l'instance EC2) comme source.

Les groupes de sécurité se réfèrent mutuellement en tant que destination et source, et autorisent uniquement le trafic sur le port de la base de données. Vous pouvez réutiliser ces groupes de sécurité de sorte que toute base de données avec le groupe de sécurité `rds-ec2-x` puisse communiquer avec toute instance EC2 avec le groupe de sécurité `ec2-rds-x`.

Les noms des groupes de sécurité suivent un modèle. Pour les groupes de sécurité créés par Amazon EC2, le modèle est `ec2-rds-x`, et pour les groupes de sécurité créés par Amazon RDS, le modèle est `rds-ec2-x`. **x** est un nombre, qui augmente de 1 chaque fois qu'un nouveau groupe de sécurité est automatiquement créé.

Tutoriel : Connexion d'une instance Amazon EC2 à une base de données Amazon RDS

Objectif du tutoriel

L'objectif de ce tutoriel est d'apprendre à configurer une connexion sécurisée entre une instance Amazon EC2 et une base de données Amazon RDS à l'aide de la AWS Management Console.

Il existe différentes options pour configurer la connexion. Dans ce tutoriel, nous explorons les trois options suivantes :

- [Option 1 : connexion automatique de votre instance EC2 à votre base de données RDS à l'aide de la console EC2](#)

Utilisez la fonction de connexion automatique de la console EC2 pour configurer automatiquement la connexion entre votre instance EC2 et votre base de données RDS afin de permettre le trafic entre l'instance EC2 et la base de données RDS.

- [Option 2 : connexion automatique de votre instance EC2 à votre base de données RDS à l'aide de la console RDS](#)

Utilisez la fonction de connexion automatique de la console RDS pour configurer automatiquement la connexion entre votre instance EC2 et votre base de données RDS afin de permettre le trafic entre l'instance EC2 et la base de données RDS.

- [Option 3 : connexion manuelle de votre instance EC2 à votre base de données RDS en imitant la fonction de connexion automatique](#)

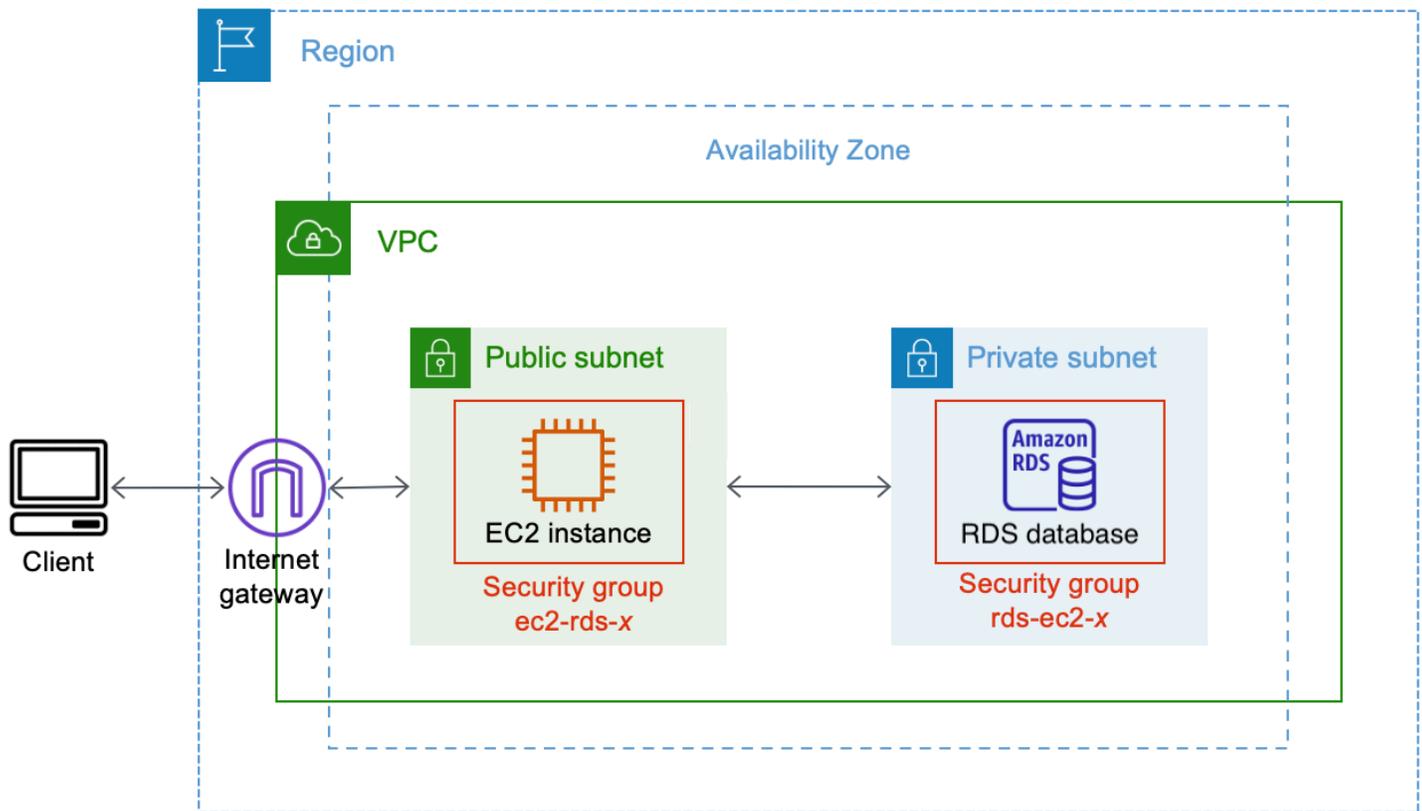
Configurez la connexion entre votre instance EC2 et votre base de données RDS en configurant et en affectant manuellement les groupes de sécurité pour reproduire la configuration créée automatiquement par la fonction de connexion automatique dans l'option 1 et l'option 2.

Contexte

Pour expliquer pourquoi vous devriez configurer une connexion entre votre instance EC2 et une base de données RDS, considérons le scénario suivant : votre site Web présente un formulaire à remplir par vos utilisateurs. Vous devez capturer les données du formulaire dans une base de données. Vous pouvez héberger votre site Web sur une instance EC2 qui a été configurée comme un serveur Web et vous pouvez capturer les données du formulaire dans une base de données RDS. L'instance EC2 et la base de données RDS doivent être connectées l'une à l'autre pour que les données du formulaire puissent passer de l'instance EC2 à la base de données RDS. Ce tutoriel explique comment configurer cette connexion. Notez que ce n'est qu'un exemple de cas d'utilisation pour connecter une instance EC2 et une base de données RDS.

Architecture

Le diagramme suivant montre les ressources créées et la configuration architecturale qui résulte de l'exécution de toutes les étapes de ce tutoriel.



Le diagramme illustre les ressources suivantes que vous allez créer :

- Vous allez créer une instance EC2 et une base de données RDS dans le même Région AWS VPC et la même zone de disponibilité.
- Vous allez créer l'instance EC2 dans un sous-réseau public.
- Vous allez créer la base de données RDS dans un sous-réseau privé.

Lorsque vous utilisez la console RDS pour créer la base de données RDS et connecter automatiquement l'instance EC2, le VPC, le groupe de sous-réseau de la base de données et les paramètres d'accès public de la base de données sont automatiquement sélectionnés. La base de données RDS est automatiquement créée dans un sous-réseau privé au sein du même VPC que l'instance EC2.

- Les utilisateurs Internet peuvent se connecter à l'instance EC2 en utilisant SSH ou HTTP/HTTPS via une passerelle Internet.
- Les utilisateurs Internet ne peuvent pas se connecter directement à la base de données RDS ; seule l'instance EC2 est connectée à la base de données RDS.

- Lorsque vous utilisez la fonction de connexion automatique pour autoriser le trafic entre l'instance EC2 et la base de données RDS, les groupes de sécurité suivants sont automatiquement créés et ajoutés :
 - Le groupe de sécurité `ec2-rds-x` est créé et ajouté à l'instance EC2. Il possède une règle sortante qui fait référence au groupe de sécurité `rds-ec2-x` comme destination. Cela permet au trafic de l'instance EC2 d'atteindre la base de données RDS avec le groupe de sécurité `rds-ec2-x`.
 - Le groupe de sécurité `rds-ec2-x` est créé et ajouté à la base de données RDS. Il possède une règle entrante qui fait référence au groupe de sécurité `ec2-rds-x` comme source. Cela permet au trafic provenant de l'instance EC2 avec le groupe de sécurité `ec2-rds-x` d'atteindre la base de données RDS.

En utilisant des groupes de sécurité distincts (un pour l'instance EC2 et un pour la base de données RDS), vous avez un meilleur contrôle sur la sécurité de l'instance et de la base de données. Si vous deviez utiliser le même groupe de sécurité sur l'instance et la base de données, puis le modifier pour qu'il convienne, par exemple, uniquement à la base de données, la modification affecterait à la fois l'instance et la base de données. En d'autres termes, si vous deviez utiliser un groupe de sécurité, vous pourriez modifier involontairement la sécurité d'une ressource (soit l'instance, soit la base de données) parce que vous auriez oublié que le groupe de sécurité y est attaché.

Les groupes de sécurité créés automatiquement respectent également le principe du moindre privilège car ils n'autorisent que la connexion mutuelle pour cette charge de travail sur le port de la base de données en créant une paire de groupes de sécurité spécifique à la charge de travail.

Considérations

Tenez compte des éléments suivants lorsque vous effectuez les tâches de ce tutoriel :

- Deux consoles : vous utiliserez les deux consoles suivantes pour ce tutoriel :
 - Console Amazon EC2 : vous utiliserez la console EC2 pour lancer des instances, pour connecter automatiquement une instance EC2 à une base de données RDS et, pour l'option manuelle, pour configurer la connexion en créant les groupes de sécurité.
 - Console Amazon RDS : vous utiliserez la console RDS pour créer une base de données RDS et pour connecter automatiquement une instance EC2 à une base de données RDS.
- Un VPC : pour utiliser la fonction de connexion automatique, votre instance EC2 et votre base de données RDS doivent se trouver dans le même VPC.

Si vous deviez configurer manuellement la connexion entre votre instance EC2 et votre base de données RDS, vous pourriez lancer votre instance EC2 dans un VPC et votre base de données RDS dans un autre VPC ; cependant, vous auriez besoin de mettre en place un routage et une configuration VPC supplémentaires. Ce scénario n'est pas décrit dans ce tutoriel.

- Un Région AWS — L'instance EC2 et la base de données RDS doivent être situées dans la même région.
- Deux groupes de sécurité : la connectivité entre l'instance EC2 et la base de données RDS est configurée par deux groupes de sécurité : un groupe de sécurité pour votre instance EC2 et un groupe de sécurité pour votre base de données RDS.

Lorsque vous utilisez la fonction de connexion automatique de la console EC2 ou la console RDS pour configurer la connectivité (option 1 et option 2 de ce tutoriel), les groupes de sécurité sont automatiquement créés et affectés à l'instance EC2 et à la base de données RDS.

Si vous n'utilisez pas la fonction de connexion automatique, vous devrez créer et affecter manuellement les groupes de sécurité. Vous le faites dans l'option 3 de ce tutoriel.

Durée du didacticiel

30 minutes

Vous pouvez suivre l'intégralité de ce tutoriel en une seule séance ou effectuer une tâche à la fois.

Coûts

En suivant ce didacticiel, les AWS ressources que vous créez peuvent vous coûter cher.

Vous pouvez utiliser Amazon EC2 dans le cadre du [niveau gratuit](#) à condition que votre AWS compte date de moins de 12 mois et que vous configuriez vos ressources conformément aux exigences du niveau gratuit.

Si votre instance EC2 et votre base de données RDS se trouvent dans des zones de disponibilité différentes, vous devrez payer des frais de transfert de données. Pour ne pas encourir ces frais, l'instance EC2 et la base de données RDS doivent se trouver dans la même zone de disponibilité. Pour plus d'informations sur les frais de transfert de données, consultez [Transfert de données](#) sur la page Tarification à la demande d'Amazon EC2.

Pour éviter d'encourir des frais après avoir terminé le tutoriel, assurez-vous de supprimer les ressources si elles ne sont plus nécessaires. Pour connaître la marche à suivre pour supprimer les ressources, consultez [Nettoyage](#).

Option 1 : connexion automatique de votre instance EC2 à votre base de données RDS à l'aide de la console EC2

Objectif

L'objectif de l'option 1 est d'explorer la fonction de connexion automatique de la console EC2 qui configure automatiquement la connexion entre votre instance EC2 et la base de données RDS pour permettre le trafic de l'instance EC2 vers la base de données RDS. L'option 3 vous permet d'apprendre à configurer manuellement la connexion.

Avant de commencer

Vous aurez besoin des éléments suivants pour compléter ce tutoriel :

- Une base de données RDS qui se trouve dans le même VPC que l'instance EC2. Vous pouvez soit utiliser une base de données RDS existante, soit suivre les étapes de la tâche 1 pour créer une nouvelle base de données RDS.
- Une instance EC2 qui se trouve dans le même VPC que la base de données RDS. Vous pouvez utiliser une instance EC2 existante ou suivre les étapes de la tâche 2 pour créer une nouvelle instance EC2.
- Des autorisations pour appeler les opérations suivantes :
 - `ec2:AssociateRouteTable`
 - `ec2:AuthorizeSecurityGroupEgress`
 - `ec2:CreateRouteTable`
 - `ec2:CreateSecurityGroup`
 - `ec2:CreateSubnet`
 - `ec2:DescribeInstances`
 - `ec2:DescribeNetworkInterfaces`
 - `ec2:DescribeRouteTables`
 - `ec2:DescribeSecurityGroups`
 - `ec2:DescribeSubnets`
 - `ec2:ModifyNetworkInterfaceAttribute`

- `ec2:RevokeSecurityGroupEgress`

Les tâches pour terminer l'option 1

- [Tâche 1 : création d'une base de données RDS – facultatif](#)
- [Tâche 2 : lancement d'une instance EC2 – facultatif](#)
- [Tâche 3 : connexion automatique de votre instance EC2 à votre base de données RDS](#)
- [Tâche 4 : vérification de la configuration de la connexion](#)

Tâche 1 : création d'une base de données RDS – facultatif

 Note

La création d'une base de données Amazon RDS n'est pas l'objet de ce tutoriel. Si vous disposez déjà d'une base de données RDS et que vous voulez l'utiliser dans ce tutoriel, vous pouvez ignorer cette tâche.

Objectif de la tâche

L'objectif de cette tâche est de créer une base de données RDS afin que vous puissiez terminer la tâche 3 où vous configurez la connexion entre votre instance EC2 et votre base de données RDS. Si vous disposez d'une base de données RDS que vous pouvez utiliser, vous pouvez sauter cette tâche.

 Important

Si vous utilisez une base de données RDS existante, assurez-vous qu'elle se trouve dans le même VPC que votre instance EC2 afin que vous puissiez utiliser la fonction de connexion automatique.

Étapes à suivre pour créer une base de données RDS

Effectuez les étapes suivantes pour créer une base de données RDS.

Pour voir une animation de ces étapes, consultez [Voir une animation : création d'une base de données RDS](#).

Configuration de la base de données RDS

Les étapes de cette tâche configurent la base de données RDS comme suit :

- Type de moteur : MySQL
- Modèle : offre gratuite
- Identifiant d'instance de base de données : **tutorial-database-1**
- Classe d'instance de base de données : `db.t3.micro`

Important

Dans un environnement de production, vous devez configurer votre base de données pour répondre à vos besoins spécifiques.

Création d'une base de données MySQL RDS

1. Ouvrez la console Amazon RDS à l'adresse <https://console.aws.amazon.com/rds/>.
2. Dans le sélecteur de région (en haut à droite), sélectionnez une Région AWS. La base de données et l'instance EC2 doivent se trouver dans la même région afin d'utiliser la fonction de connexion automatique de la console EC2.
3. Dans le tableau de bord, choisissez Create database (Créer une base de données).
4. Sous Choose a database creation method (Choisir une méthode de création de base de données), vérifiez que l'option Standard create (Création standard) est sélectionnée. Si vous choisissez Easy create (Création facile), le sélecteur de VPC n'est pas disponible. Vous devez vous assurer que votre base de données se trouve dans le même VPC que votre instance EC2 afin d'utiliser la fonction de connexion automatique de la console EC2.
5. Sous Engine options (Options du moteur), pour Engine type (Type de moteur), choisissez MySQL.
6. Sous Templates (Modèles), choisissez un exemple de modèle pour répondre à vos besoins. Pour ce tutoriel, choisissez Free tier (Offre gratuite) pour créer une base de données sans frais. Toutefois, notez que l'offre gratuite n'est disponible que si votre compte a moins de 12 mois. D'autres restrictions s'appliquent. Vous pouvez en savoir plus en cliquant sur le lien Info dans la case Free tier (Offre gratuite).
7. Sous Paramètres, effectuez l'une des actions suivantes :

- a. Pour DB instance identifier (Identifiant d'instance de base de données), saisissez un nom pour la base de données. Dans le cadre de ce didacticiel, entrez **tutorial-database-1**.
 - b. Pour Master username (Nom d'utilisateur principal), laissez le nom par défaut, qui est **admin**.
 - c. Pour Master password (Mot de passe principal), saisissez un mot de passe dont vous pouvez vous souvenir pour ce tutoriel, puis, pour Confirm password (Confirmer le mot de passe), saisissez à nouveau le mot de passe.
8. Sous Instance configuration (Configuration de l'instance), pour DB instance class (Classe d'instance de base de données), laissez la valeur par défaut, qui est db.t3.micro. Si votre compte a moins de 12 mois, vous pouvez utiliser cette classe de base de données gratuitement. D'autres restrictions s'appliquent. Pour plus d'informations, consultez la page sur l'[offre gratuite AWS](#).
9. Sous Connectivity (Connectivité), pour Compute resource (Ressource de calcul), choisissez Don't connect to an EC2 compute resource (Ne pas se connecter à une ressource de calcul EC2), car vous connecterez l'instance EC2 et la base de données RDS plus tard dans la tâche 3.

(Plus tard, dans l'option 2 de ce tutoriel, vous testerez la fonction de connexion automatique dans la console RDS en choisissant Connect to an EC2 compute resource (Se connecter à une ressource de calcul EC2).)

10. Pour Virtual private cloud (VPC) (Cloud privé virtuel (VPC)), choisissez un VPC. Le VPC doit avoir un groupe de sous-réseau de base de données. Pour utiliser la fonction de connexion automatique, votre instance EC2 et votre base de données RDS doivent se trouver dans le même VPC.
11. Conservez toutes les valeurs par défaut pour les autres champs de cette page.
12. Choisissez Créer une base de données.

Sur l'écran Databases (Bases de données), le Status (Statut) de la nouvelle base de données est Creating (Création) jusqu'à ce que la base de données soit prête à être utilisée. Lorsque le statut passe à Available (Disponible), vous pouvez vous connecter à la base de données. En fonction de la classe de base de données et de la quantité de stockage, la mise à disposition de la nouvelle base de données peut prendre jusqu'à 20 minutes.

Voir une animation : création d'une base de données RDS

The screenshot shows the Amazon RDS console dashboard. On the left is a navigation menu with options like Databases, Performance insights, Snapshots, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Events, Event subscriptions, and Certificate update. The main content area features a top banner with a 'Create database' button and a 'Resources' section listing various RDS resources and their usage in the EU (Stockholm) region. Below the resources is another 'Create database' section.

Amazon RDS ×

Dashboard

- Databases
- Performance insights
- Snapshots
- Automated backups
- Reserved instances
- Proxies

- Subnet groups
- Parameter groups
- Option groups
- Custom engine versions

- Events
- Event subscriptions

- Certificate update

Try the new Amazon RDS Multi-AZ deployment option for MySQL and PostgreSQL
For your Amazon RDS for MySQL and PostgreSQL workloads, improve transactional commit latencies instances by deploying the Multi-AZ DB cluster [Learn more](#)

Create database

Or, [Restore Multi-AZ DB Cluster from Snapshot](#)

Resources

You are using the following Amazon RDS resources in the EU (Stockholm) region (used/quota)

DB Instances (3/40) Allocated storage (0.3 TB/100 TB) Increase DB Instances limit	Parameter groups (2) Default (2) Custom (0/100)
DB Clusters (1/40)	Option groups (1) Default (1) Custom (0/20)
Reserved instances (0/40)	Subnet groups (1/50)
Snapshots (1)	Supported platforms VPC
Manual	Default network vpc-78678c
DB Cluster (0/100)	
DB Instance (0/100)	
Automated	
DB Cluster (1)	
DB Instance (0)	
Recent events (5)	
Event subscriptions (0/20)	

Create database

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database i

Voici le moment pour [Tâche 2 : lancement d'une instance EC2 – facultatif](#).

Tâche 2 : lancement d'une instance EC2 – facultatif

Note

Le lancement d'une instance n'est pas l'objet de ce tutoriel. Si vous disposez déjà d'une instance Amazon EC2 et que vous voulez l'utiliser dans ce tutoriel, vous pouvez ignorer cette tâche.

Objectif de la tâche

L'objectif de cette tâche est de lancer une instance EC2 afin que vous puissiez terminer la tâche 3 où vous configurez la connexion entre votre instance EC2 et votre base de données Amazon RDS. Si vous disposez d'une instance EC2 que vous pouvez utiliser, vous pouvez sauter cette tâche.

Important

Si vous utilisez une instance EC2 existante, assurez-vous qu'elle se trouve dans le même VPC que votre base de données RDS afin que vous puissiez utiliser la fonction de connexion automatique.

Étapes pour lancer une instance EC2

Effectuez les étapes suivantes pour lancer une instance EC2 pour ce tutoriel.

Pour voir une animation de ces étapes, consultez [Voir une animation : lancement d'une instance EC2](#).

Configuration des instances EC2

Les étapes de cette tâche configurent l'instance EC2 comme suit :

- Nom de l'instance : **tutorial-instance-1**
- AMI : Amazon Linux 2
- Type d'instance : `t2.micro`
- Attribuer automatiquement l'adresse IP publique : Activé
- Groupe de sécurité avec les trois règles suivantes :
 - Autoriser SSH depuis votre adresse IP
 - Autoriser le trafic HTTPS depuis n'importe où
 - Autoriser le trafic HTTP depuis n'importe où

Important

Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

Pour lancer une instance EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le sélecteur de région (en haut à droite), sélectionnez une Région AWS. L'instance et la base de données RDS doivent se trouver dans la même région afin d'utiliser la fonction de connexion automatique de la console EC2.
3. Dans EC2 Dashboard (Tableau de bord EC2), choisissez Launch instance (Lancer l'instance).
4. Sous Name and tags (Noms et balises), pour Name (Nom), saisissez un nom pour identifier votre instance. Pour ce tutoriel, nommez l'instance **tutorial-instance-1**. Bien que le nom de l'instance ne soit pas obligatoire, lorsque vous sélectionnez votre instance dans la console EC2, le nom vous aidera à l'identifier facilement.
5. Sous Application and OS Images (Images de l'application et du système d'exploitation), choisissez une AMI qui répond aux besoins de votre serveur Web. Ce tutoriel utilise Amazon Linux 2.
6. Sous Instance type (Type d'instance), pour Instance type (Type d'instance), sélectionnez un type d'instance qui répond aux besoins de votre serveur Web. Ce tutoriel utilise t2.micro.

Note

Vous pouvez utiliser Amazon EC2 dans le cadre du [niveau gratuit](#) à condition que votre AWS compte date de moins de 12 mois et que vous choisissiez un type d't2.microinstance (ou t3.micro dans les régions où ce type d'instance n't2.microest pas disponible).

7. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez votre paire de clés.
8. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :
 - a. Pour Network (Réseau) et Subnet (Sous-réseau), si vous n'avez pas apporté de modifications à votre VPC ou à vos sous-réseaux par défaut, vous pouvez conserver les paramètres par défaut.

Si vous avez apporté des modifications à votre VPC ou à vos sous-réseaux par défaut, vérifiez ce qui suit :

- i. L'instance doit se trouver dans le même VPC que la base de données RDS pour utiliser la fonction de connexion automatique. Par défaut, vous n'avez qu'un seul VPC.

- ii. Le VPC dans lequel vous lancez votre instance doit avoir une passerelle Internet qui lui est attachée afin que vous puissiez accéder à votre serveur Web depuis Internet. Votre VPC par défaut est automatiquement configuré avec une passerelle Internet.
 - iii. Pour vous assurer que votre instance reçoit une adresse IP publique, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), vérifiez que Enable (Activer) est sélectionné. Si l'option Disable (Désactiver) est sélectionnée, choisissez Edit (Modifier) (à droite de Network Settings (Paramètres réseau)), puis, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), choisissez Enable (Activer).
 - b. Pour vous connecter à votre instance en utilisant SSH, vous avez besoin d'une règle de groupe de sécurité qui autorise le trafic SSH (Linux) ou RDP (Windows) à partir de l'adresse IPv4 publique de votre ordinateur. Par défaut, lorsque vous lancez une instance, un nouveau groupe de sécurité est créé avec une règle qui autorise le trafic SSH entrant de n'importe où.

Pour vous assurer que seule votre adresse IP peut se connecter à votre instance, sous Firewall (security groups) (Pare-feu (groupes de sécurité)), dans la liste déroulante située à côté de la case Allow SSH traffic from (Autoriser le trafic SSH depuis), choisissez My IP (Mon adresse IP).
 - c. Pour autoriser le trafic depuis Internet vers votre instance, cochez les cases suivantes :
 - Allow HTTPs traffic from the internet (Autoriser le trafic HTTPs depuis Internet)
 - Allow HTTP traffic from the internet (Autoriser le trafic HTTP depuis Internet)
9. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance).
 10. Gardez la page de confirmation ouverte. Vous en aurez besoin pour la tâche suivante lorsque vous connecterez automatiquement votre instance à votre base de données.

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à `terminated` au lieu de `running`, consultez [Résoudre les problèmes de lancement d'instance](#).

Pour plus d'informations sur le lancement d'une instance, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Voir une animation : lancement d'une instance EC2

Resources

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	2	Dedicated Hosts	0	Elastic IPs	0
Instances	2	Key pairs	1	Load balancers	0
Placement groups	0	Security groups	10	Snapshots	1
Volumes	3				

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) [Migrate a server](#)

Note: Your instances will launch in the Europe (Stockholm) Region

Scheduled events

Europe (Stockholm)
No scheduled events

Service health

Region: Europe (Stockholm)
Status: ✔ This service is operating normally

Zones

Zone name	Zone ID
eu-north-1a	eun1-az1
eu-north-1b	eun1-az2
eu-north-1c	eun1-az3

Voici le moment pour [Tâche 3 : connexion automatique de votre instance EC2 à votre base de données RDS](#).

Tâche 3 : connexion automatique de votre instance EC2 à votre base de données RDS

Objectif de la tâche

L'objectif de cette tâche est d'utiliser la fonction de connexion automatique de la console EC2 pour configurer automatiquement la connexion entre votre instance EC2 et votre base de données RDS.

Étapes pour connecter votre instance EC2 et votre base de données RDS

Effectuez les étapes suivantes pour connecter votre instance EC2 et votre base de données RDS à l'aide de la fonction de connexion automatique de la console EC2.

Pour voir une animation de ces étapes, consultez [Voir une animation : Connexion automatique d'une instance EC2 nouvellement lancée à une base de données RDS](#).

Connexion automatique d'une instance EC2 à une base de données RDS à l'aide de la console EC2

1. Sur la page de confirmation du lancement de l'instance (elle doit être ouverte depuis la tâche précédente), choisissez Connect an RDS database (Connecter une base de données RDS).

Si vous avez fermé la page de confirmation, suivez ces étapes :

- a. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
- b. Dans le panneau de navigation, sélectionnez Instances.
- c. Sélectionnez l'instance EC2 que vous venez de créer, puis choisissez Actions, Networking (Réseaux), Connect an RDS database (Connecter une base de données RDS).

Si Connect RDS database (Connecter la base de données RDS) n'est pas disponible, vérifiez que l'instance EC2 est dans l'état Running (En cours d'exécution).

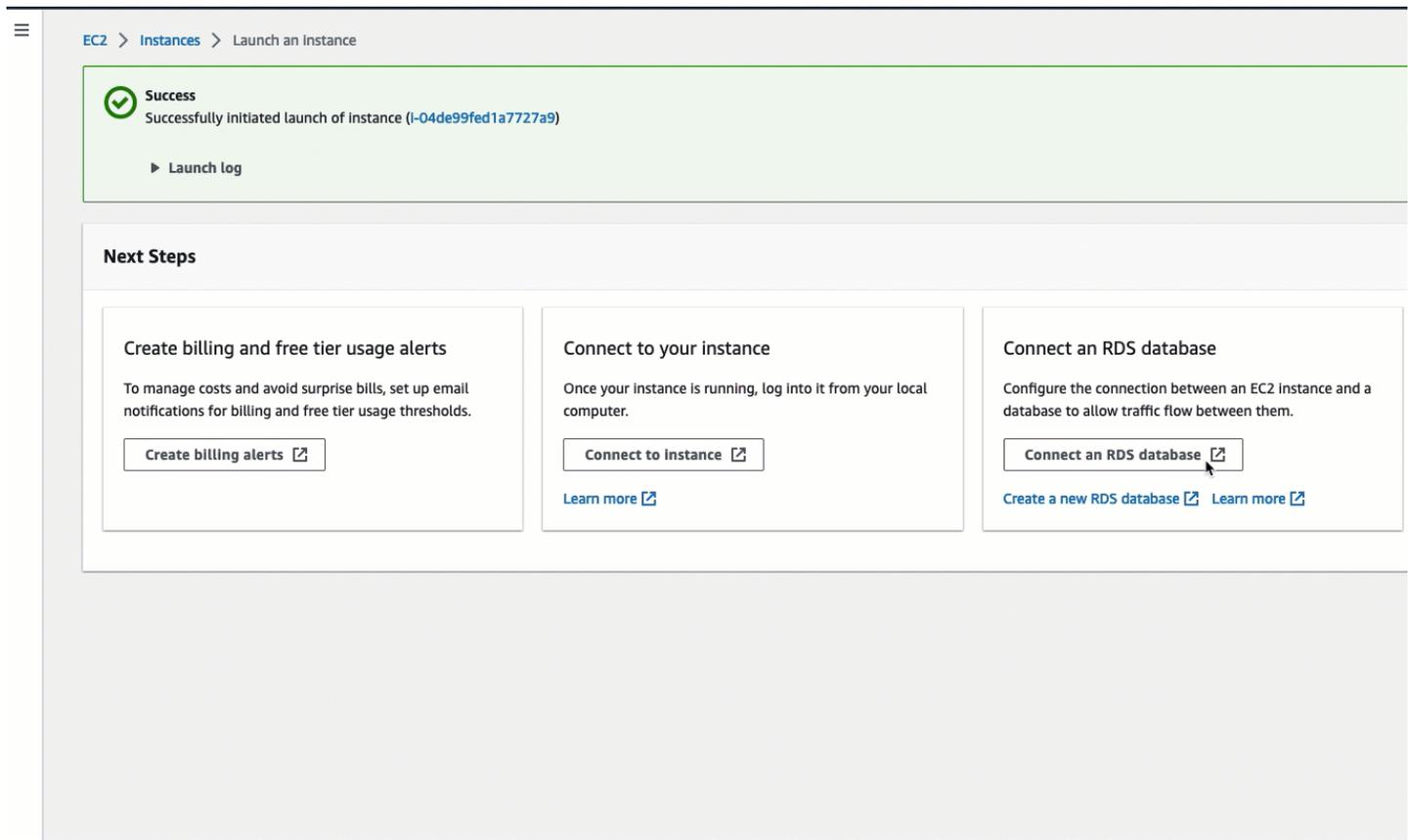
2. Pour Database role (Rôle de la base de données), choisissez Instance. Dans ce cas, Instance fait référence à l'instance de la base de données.
3. Pour RDS database (Base de données RDS), choisissez la base de données RDS que vous avez créée dans la tâche 1.

Note

L'instance EC2 et la base de données RDS doivent se trouver dans le même VPC pour pouvoir se connecter l'une à l'autre.

4. Choisissez Se connecter.

Voir une animation : Connexion automatique d'une instance EC2 nouvellement lancée à une base de données RDS



The screenshot shows the Amazon EC2 console interface. At the top, there is a navigation breadcrumb: EC2 > Instances > Launch an Instance. Below this, a green success message box states: "Success Successfully initiated launch of instance (i-04de99fed1a7727a9)" with a "Launch log" link. Underneath, a "Next Steps" section contains three cards:

- Create billing and free tier usage alerts**: "To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds." Includes a "Create billing alerts" button.
- Connect to your instance**: "Once your instance is running, log into it from your local computer." Includes a "Connect to instance" button and a "Learn more" link.
- Connect an RDS database**: "Configure the connection between an EC2 Instance and a database to allow traffic flow between them." Includes a "Connect an RDS database" button, a "Create a new RDS database" link, and a "Learn more" link.

Voici le moment pour [Tâche 4 : vérification de la configuration de la connexion](#).

Tâche 4 : vérification de la configuration de la connexion

Objectif de la tâche

L'objectif de cette tâche est de vérifier que les deux groupes de sécurité ont été créés et affectés à l'instance et à la base de données.

Lorsque vous utilisez la fonction de connexion automatique de la console EC2 pour configurer la connectivité, les groupes de sécurité sont automatiquement créés et affectés à l'instance et à la base de données, comme suit :

- Le groupe de sécurité `rds-ec2-x` est créé et ajouté à la base de données RDS. Il possède une règle entrante qui fait référence au groupe de sécurité `ec2-rds-x` comme source. Cela permet au trafic provenant de l'instance EC2 avec le groupe de sécurité `ec2-rds-x` d'atteindre la base de données RDS.

- Le groupe de sécurité `ec2-rds-x` est créé et ajouté à l'instance EC2. Il possède une règle sortante qui fait référence au groupe de sécurité `rds-ec2-x` comme destination. Cela permet au trafic de l'instance EC2 d'atteindre la base de données RDS avec le groupe de sécurité `rds-ec2-x`.

Étapes à suivre pour vérifier la configuration de la connexion

Effectuez les étapes suivantes pour vérifier la configuration de la connexion.

Pour voir une animation de ces étapes, consultez [Voir une animation : vérification de la configuration de la connexion](#).

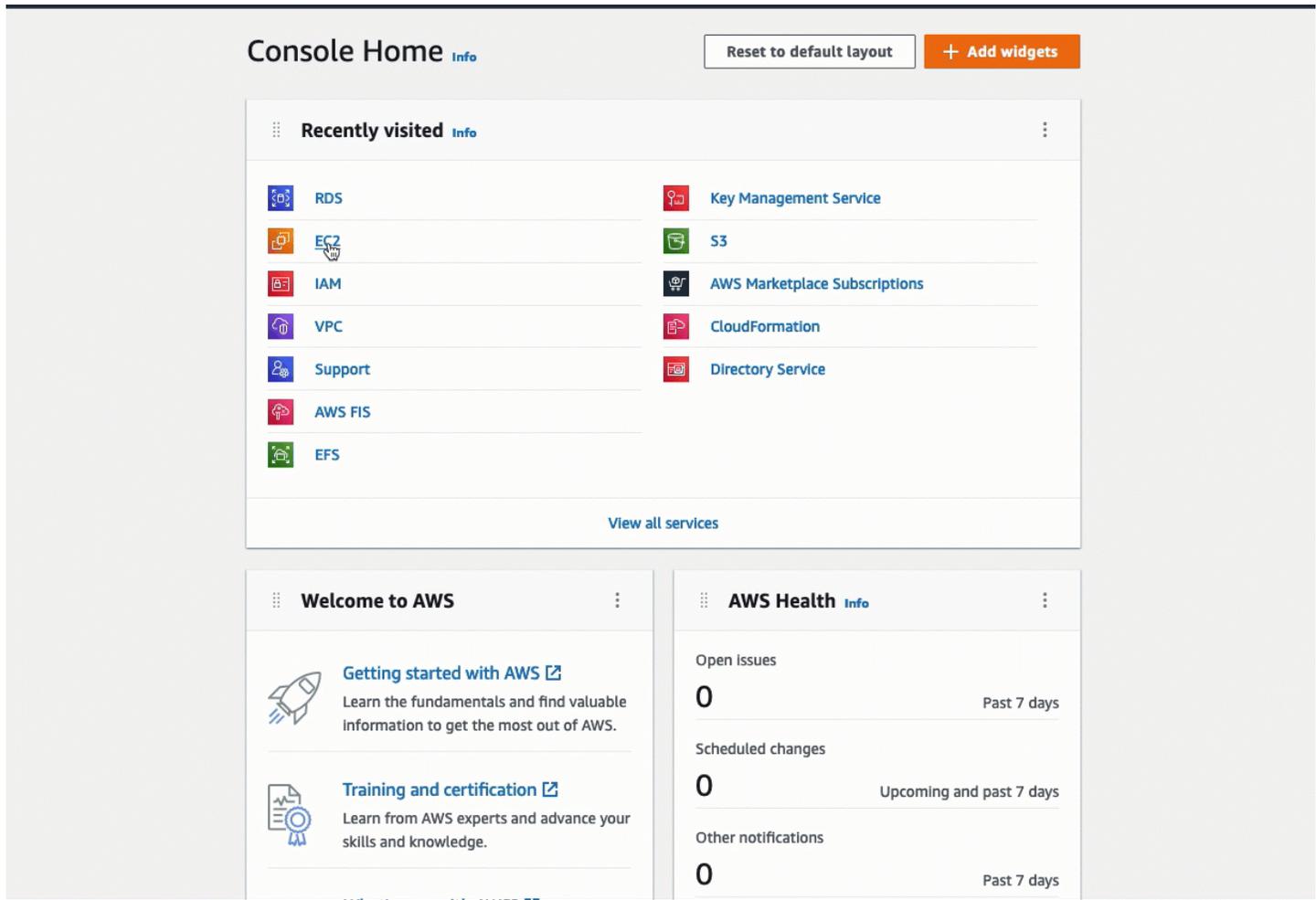
Pour vérifier la configuration de la connexion à l'aide de la console

1. Ouvrez la console Amazon RDS à l'adresse <https://console.aws.amazon.com/rds/>.
2. Dans la page de navigation, choisissez Databases (Bases de données).
3. Choisissez la base de données RDS que vous avez créée pour ce tutoriel.
4. Dans l'onglet Connectivity & security (Connectivité et sécurité), sous Security (Sécurité), VPC security groups (Groupes de sécurité VPC), vérifiez qu'un groupe de sécurité appelé `rds-ec2-x` est affiché.
5. Sélectionnez le groupe de sécurité `rds-ec2-x`. L'écran Security Groups (Groupes de sécurité) de la console EC2 s'ouvre.
6. Sélectionnez le groupe de sécurité `rds-ec2-x` pour l'ouvrir.
7. Choisissez l'onglet Inbound rules (Règles entrantes).
8. Vérifiez que la règle de groupe de sécurité suivante existe :
 - Type : MySQL/Aurora
 - Plage de ports : 3306
 - Source : **`sg-0987654321example`** / `ec2-rds-x` : il s'agit du groupe de sécurité qui est attribué à l'instance EC2 que vous avez vérifiée dans les étapes précédentes.
 - Description : Règle pour autoriser les connexions des instances EC2 avec **`sg-1234567890example`** attaché
9. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
10. Dans le panneau de navigation, sélectionnez Instances.
11. Choisissez l'instance EC2 que vous avez sélectionnée pour vous connecter à la base de données RDS dans la tâche précédente, puis choisissez l'onglet Security (Sécurité).

12. Sous Security details (Détails de sécurité), Security groups (Groupes de sécurité), vérifiez qu'un groupe de sécurité appelé ec2-rds-**x** figure dans la liste. **x** est un nombre.
13. Sélectionnez le groupe de sécurité ec2-rds-**x** pour l'ouvrir.
14. Choisissez l'onglet Outbound rules (Règles sortantes).
15. Vérifiez que la règle de groupe de sécurité suivante existe :
 - Type : MySQL/Aurora
 - Plage de ports : 3306
 - Destination : **sg-1234567890example** / rds-ec2-**x**
 - Description : Règle pour autoriser les connexions à **database-tutorial** à partir de n'importe quelle instance à laquelle ce groupe de sécurité est attaché

En vérifiant que ces groupes de sécurité et ces règles de groupe de sécurité existent et qu'ils sont affectés à la base de données RDS et à l'instance EC2 comme décrit dans cette procédure, vous pouvez vérifier que la connexion a été automatiquement configurée en utilisant la fonction de connexion automatique.

Voir une animation : vérification de la configuration de la connexion



Vous avez terminé l'option 1 de ce tutoriel. Vous pouvez désormais soit terminer l'option 2, qui vous apprend à utiliser la console RDS pour connecter automatiquement une instance EC2 à une base de données RDS, soit terminer l'option 3, qui vous apprend à configurer manuellement les groupes de sécurité qui ont été créés automatiquement dans l'option 1.

Option 2 : connexion automatique de votre instance EC2 à votre base de données RDS à l'aide de la console RDS

Objectif

L'objectif de l'option 2 est d'explorer la fonction de connexion automatique de la console RDS qui configure automatiquement la connexion entre votre instance EC2 et la base de données RDS pour permettre le trafic de l'instance EC2 vers la base de données RDS. L'option 3 vous permet d'apprendre à configurer manuellement la connexion.

Avant de commencer

Vous aurez besoin des éléments suivants pour compléter ce tutoriel :

- Une instance EC2 qui se trouve dans le même VPC que la base de données RDS. Vous pouvez utiliser une instance EC2 existante ou suivre les étapes de la tâche 1 pour créer une nouvelle instance.
- Des autorisations pour appeler les opérations suivantes :
 - `ec2:AssociateRouteTable`
 - `ec2:AuthorizeSecurityGroupEgress`
 - `ec2:CreateRouteTable`
 - `ec2:CreateSecurityGroup`
 - `ec2:CreateSubnet`
 - `ec2:DescribeInstances`
 - `ec2:DescribeNetworkInterfaces`
 - `ec2:DescribeRouteTables`
 - `ec2:DescribeSecurityGroups`
 - `ec2:DescribeSubnets`
 - `ec2:ModifyNetworkInterfaceAttribute`
 - `ec2:RevokeSecurityGroupEgress`

Les tâches pour terminer l'option 2

- [Tâche 1 : lancement d'une instance EC2 – facultatif](#)
- [Tâche 2 : création d'une base de données RDS et connexion automatique à votre instance EC2](#)
- [Tâche 3 : vérification de la configuration de la connexion](#)

Tâche 1 : lancement d'une instance EC2 – facultatif

Note

Le lancement d'une instance n'est pas l'objet de ce tutoriel. Si vous disposez déjà d'une instance Amazon EC2 et que vous voulez l'utiliser dans ce tutoriel, vous pouvez ignorer cette tâche.

Objectif de la tâche

L'objectif de cette tâche est de lancer une instance EC2 afin que vous puissiez terminer la tâche 2 où vous configurez la connexion entre votre instance EC2 et votre base de données Amazon RDS. Si vous disposez d'une instance EC2 que vous pouvez utiliser, vous pouvez sauter cette tâche.

Étapes pour lancer une instance EC2

Effectuez les étapes suivantes pour lancer une instance EC2 pour ce tutoriel.

Pour voir une animation de ces étapes, consultez [Voir une animation : lancement d'une instance EC2](#).

Configuration des instances EC2

Les étapes de cette tâche configurent l'instance EC2 comme suit :

- Nom de l'instance : **tutorial-instance-2**
- AMI : Amazon Linux 2
- Type d'instance : `t2.micro`
- Attribuer automatiquement l'adresse IP publique : Activé
- Groupe de sécurité avec les trois règles suivantes :
 - Autoriser SSH depuis votre adresse IP
 - Autoriser le trafic HTTPS depuis n'importe où
 - Autoriser le trafic HTTP depuis n'importe où

Important

Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

Pour lancer une instance EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans EC2 Dashboard (Tableau de bord EC2), choisissez Launch instance (Lancer l'instance).
3. Sous Name and tags (Noms et balises), pour Name (Nom), saisissez un nom pour identifier votre instance. Pour ce tutoriel, nommez l'instance **tutorial-instance-2**. Bien que le nom de

l'instance ne soit pas obligatoire, lorsque vous sélectionnez votre instance dans la console RDS, le nom vous aidera à l'identifier facilement.

4. Sous Application and OS Images (Images de l'application et du système d'exploitation), choisissez une AMI qui répond aux besoins de votre serveur Web. Ce tutoriel utilise Amazon Linux.
5. Sous Instance type (Type d'instance), pour Instance type (Type d'instance), sélectionnez un type d'instance qui répond aux besoins de votre serveur Web. Ce tutoriel utilise `t2.micro`.

 Note

Vous pouvez utiliser Amazon EC2 dans le cadre du [niveau gratuit](#) à condition que votre AWS compte date de moins de 12 mois et que vous choisissiez un type d'`t2.microinstance` (ou `t3.micro` dans les régions où ce type d'instance n'`t2.micro`est pas disponible).

6. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez votre paire de clés.
7. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :
 - a. Pour Network (Réseau) et Subnet (Sous-réseau), si vous n'avez pas apporté de modifications à votre VPC ou à vos sous-réseaux par défaut, vous pouvez conserver les paramètres par défaut.

Si vous avez apporté des modifications à votre VPC ou à vos sous-réseaux par défaut, vérifiez ce qui suit :

- i. L'instance doit se trouver dans le même VPC que la base de données RDS pour utiliser la configuration de connexion automatique. Par défaut, vous n'avez qu'un seul VPC.
- ii. Le VPC dans lequel vous lancez votre instance doit avoir une passerelle Internet qui lui est attachée afin que vous puissiez accéder à votre serveur Web depuis Internet. Votre VPC par défaut est automatiquement configuré avec une passerelle Internet.
- iii. Pour vous assurer que votre instance reçoit une adresse IP publique, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), vérifiez que Enable (Activer) est sélectionné. Si l'option Disable (Désactiver) est sélectionnée, choisissez Edit (Modifier) (à droite de Network Settings (Paramètres réseau)), puis, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), choisissez Enable (Activer).

- b. Pour vous connecter à votre instance en utilisant SSH, vous avez besoin d'une règle de groupe de sécurité qui autorise le trafic SSH (Linux) ou RDP (Windows) à partir de l'adresse IPv4 publique de votre ordinateur. Par défaut, lorsque vous lancez une instance, un nouveau groupe de sécurité est créé avec une règle qui autorise le trafic SSH entrant de n'importe où.

Pour vous assurer que seule votre adresse IP peut se connecter à votre instance, sous Firewall (security groups) (Pare-feu (groupes de sécurité)), dans la liste déroulante située à côté de la case Allow SSH traffic from (Autoriser le trafic SSH depuis), choisissez My IP (Mon adresse IP).

- c. Pour autoriser le trafic depuis Internet vers votre instance, cochez les cases suivantes :
 - Allow HTTPs traffic from the internet (Autoriser le trafic HTTPs depuis Internet)
 - Allow HTTP traffic from the internet (Autoriser le trafic HTTP depuis Internet)
8. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance).
9. Sélectionnez View all instances (Afficher toutes les instances) pour fermer la page de confirmation et revenir à la console. Votre instance sera d'abord dans un état pending, puis passera à l'état running.

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à terminated au lieu de running, consultez [Résoudre les problèmes de lancement d'instance](#).

Pour plus d'informations sur le lancement d'une instance, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Voir une animation : lancement d'une instance EC2

Resources

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	2	Dedicated Hosts	0	Elastic IPs	0
Instances	2	Key pairs	1	Load balancers	0
Placement groups	0	Security groups	10	Snapshots	1
Volumes	3				

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) [Migrate a server](#)

Note: Your instances will launch in the Europe (Stockholm) Region

Scheduled events

Europe (Stockholm)
No scheduled events

Service health

Region: Europe (Stockholm)
Status: ✔ This service is operating normally

Zones

Zone name	Zone ID
eu-north-1a	eun1-az1
eu-north-1b	eun1-az2
eu-north-1c	eun1-az3

Voici le moment pour [Tâche 2 : création d'une base de données RDS et connexion automatique à votre instance EC2](#).

Tâche 2 : création d'une base de données RDS et connexion automatique à votre instance EC2

Objectif de la tâche

L'objectif de cette tâche est de créer une base de données RDS et d'utiliser la fonction de connexion automatique de la console RDS pour configurer automatiquement la connexion entre votre instance EC2 et votre base de données RDS.

Étapes à suivre pour créer une base de données RDS

Effectuez les étapes suivantes pour créer une base de données RDS et la connecter à votre instance EC2 à l'aide de la fonction de connexion automatique de la console RDS.

Pour voir une animation de ces étapes, consultez [Voir une animation : création d'une base de données RDS et sa connexion automatique à une instance EC2](#).

Configuration de l'instance de base de données

Les étapes de cette tâche configurent l'instance de base de données comme suit :

- Type de moteur : MySQL
- Modèle : offre gratuite
- Identifiant d'instance de base de données : **tutorial-database**
- Classe d'instance de base de données : `db.t3.micro`

Important

Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

Pour créer une base de données RDS et la connecter automatiquement à une instance EC2

1. Ouvrez la console Amazon RDS à l'adresse <https://console.aws.amazon.com/rds/>.
2. Dans le sélecteur de région (en haut à droite), choisissez l'instance Région AWS dans laquelle vous avez créé l'instance EC2. L'instance EC2 et la base de données RDS doivent être situées dans la même région.
3. Dans le tableau de bord, choisissez Create database (Créer une base de données).
4. Sous Choose a database creation method (Choisir une méthode de création de base de données), vérifiez que l'option Standard create (Création standard) est sélectionnée. Si vous choisissez Easy create (Création facile), la fonction de connexion automatique n'est pas disponible.
5. Sous Engine options (Options du moteur), pour Engine type (Type de moteur), choisissez MySQL.
6. Sous Templates (Modèles), choisissez un exemple de modèle pour répondre à vos besoins. Pour ce tutoriel, choisissez Free tier (Offre gratuite) pour créer une base de données RDS sans frais. Toutefois, notez que l'offre gratuite n'est disponible que si votre compte a moins de 12 mois. D'autres restrictions s'appliquent. Vous pouvez en savoir plus en cliquant sur le lien Info dans la case Free tier (Offre gratuite).
7. Sous Paramètres, effectuez l'une des actions suivantes :

- a. Pour DB instance identifier (Identifiant d'instance de base de données), saisissez un nom pour la base de données. Dans le cadre de ce didacticiel, entrez **tutorial-database**.
 - b. Pour Master username (Nom d'utilisateur principal), laissez le nom par défaut, qui est **admin**.
 - c. Pour Master password (Mot de passe principal), saisissez un mot de passe dont vous pouvez vous souvenir pour ce tutoriel, puis, pour Confirm password (Confirmer le mot de passe), saisissez à nouveau le mot de passe.
8. Sous Instance configuration (Configuration de l'instance), pour DB instance class (Classe d'instance de base de données), laissez la valeur par défaut, qui est db.t3.micro. Si votre compte a moins de 12 mois, vous pouvez utiliser cette instance gratuitement. D'autres restrictions s'appliquent. Pour plus d'informations, consultez la page sur [l'offre gratuite AWS](#).
 9. Sous Connectivity (Connectivité), pour Compute resource (Ressource de calcul), choisissez Connect to an EC2 compute resource (Se connecter à une ressource de calcul EC2). Il s'agit de la fonction de connexion automatique dans la console RDS.
 10. Pour EC2 instance (Instance EC2), choisissez l'instance EC2 à laquelle vous voulez vous connecter. Pour les besoins de ce tutoriel, vous pouvez choisir l'instance que vous avez créée dans la tâche précédente, que vous avez nommée **tutorial-instance**, ou choisir une autre instance existante. Si vous ne voyez pas votre instance dans la liste, choisissez l'icône d'actualisation à droite de Connectivity (Connectivité).

Lorsque vous utilisez la fonction de connexion automatique, un groupe de sécurité est ajouté à cette instance EC2 et un autre groupe de sécurité est ajouté à la base de données RDS. Les groupes de sécurité sont automatiquement configurés pour autoriser le trafic entre l'instance EC2 et la base de données RDS. Dans la tâche suivante, vous vérifierez que les groupes de sécurité ont été créés et affectés à l'instance EC2 et à la base de données RDS.

11. Choisissez Créer une base de données.

Sur l'écran Databases (Bases de données), le Status (Statut) de la nouvelle base de données est Creating (Création) jusqu'à ce que la base de données soit prête à être utilisée. Lorsque le statut passe à Available (Disponible), vous pouvez vous connecter à la base de données. En fonction de la classe de base de données et de la quantité de stockage, la mise à disposition de la nouvelle base de données peut prendre jusqu'à 20 minutes.

Pour en savoir plus, consultez [Configurer la connectivité réseau automatique avec une instance EC2](#) dans le Guide de l'utilisateur Amazon RDS.

Voir une animation : création d'une base de données RDS et sa connexion automatique à une instance EC2

Amazon RDS ×

Dashboard

- Databases
- Performance Insights
- Snapshots
- Automated backups
- Reserved instances
- Proxies

- Subnet groups
- Parameter groups
- Option groups
- Custom engine versions

- Events
- Event subscriptions

- Certificate update

Try the new Amazon RDS Multi-AZ deployment option for MySQL and PostgreSQL
 For your Amazon RDS for MySQL and PostgreSQL workloads, improve transactional instances by deploying the Multi-AZ DB cluster [Learn more](#)

Create database

Or, [Restore Multi-AZ DB Cluster from Snapshot](#)

Resources

You are using the following Amazon RDS resources in the EU (Stockholm) region (used/quotas):

DB Instances (5/40)	Parameter Groups (0/10)
Allocated storage (0.34 TB/100 TB)	Default
Increase DB Instances limit	Custom
DB Clusters (1/40)	Option Groups (0/10)
Reserved Instances (0/40)	Default
Snapshots (2)	Custom
Manual	Subnet Groups (0/10)
DB Cluster (0/100)	Supported
DB Instance (0/100)	Default network
Automated	
DB Cluster (1)	
DB Instance (1)	
Recent events (10)	
Event subscriptions (0/20)	

Create database

Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale a rel

Voici le moment pour [Tâche 3 : vérification de la configuration de la connexion](#).

Tâche 3 : vérification de la configuration de la connexion

Objectif de la tâche

L'objectif de cette tâche est de vérifier que les deux groupes de sécurité ont été créés et affectés à l'instance et à la base de données.

Lorsque vous utilisez la fonction de connexion automatique de la console RDS pour configurer la connectivité, les groupes de sécurité sont automatiquement créés et affectés à l'instance et à la base de données, comme suit :

- Le groupe de sécurité `rds-ec2-x` est créé et ajouté à la base de données RDS. Il possède une règle entrante qui fait référence au groupe de sécurité `ec2-rds-x` comme source. Cela permet au trafic provenant de l'instance EC2 avec le groupe de sécurité `ec2-rds-x` d'atteindre la base de données RDS.
- Le groupe de sécurité `ec2-rds-x` est créé et ajouté à l'instance EC2. Il possède une règle sortante qui fait référence au groupe de sécurité `rds-ec2-x` comme destination. Cela permet au trafic de l'instance EC2 d'atteindre la base de données RDS avec le groupe de sécurité `rds-ec2-x`.

Étapes à suivre pour vérifier la configuration de la connexion

Effectuez les étapes suivantes pour vérifier la configuration de la connexion.

Pour voir une animation de ces étapes, consultez [Voir une animation : vérification de la configuration de la connexion](#).

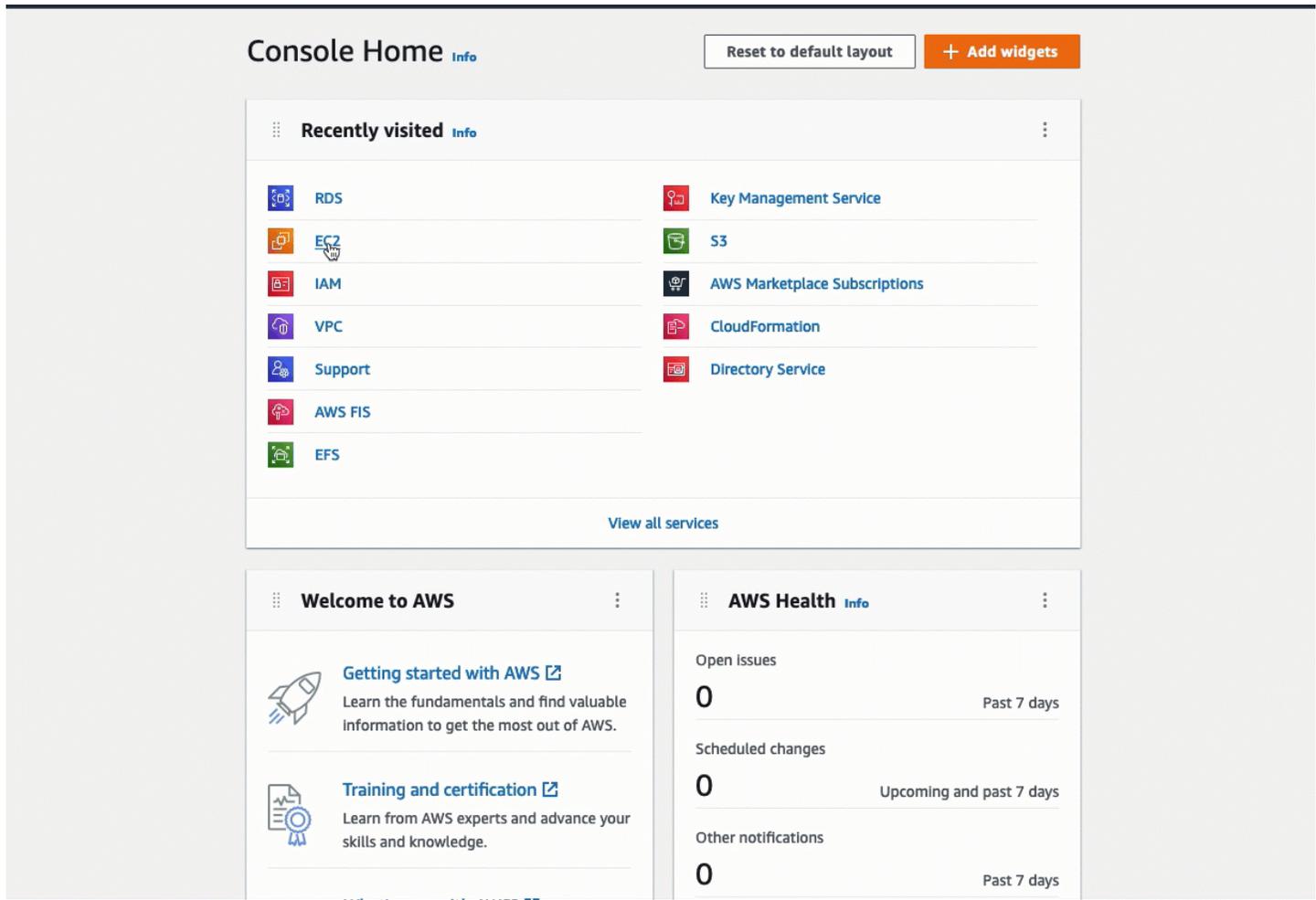
Pour vérifier la configuration de la connexion à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Choisissez l'instance EC2 que vous avez sélectionnée pour vous connecter à la base de données RDS dans la tâche précédente, puis choisissez l'onglet Security (Sécurité).
4. Sous Security details (Détails de sécurité), Security groups (Groupes de sécurité), vérifiez qu'un groupe de sécurité appelé `ec2-rds-x` figure dans la liste. **x** est un nombre.
5. Sélectionnez le groupe de sécurité `ec2-rds-x` pour l'ouvrir.
6. Choisissez l'onglet Outbound rules (Règles sortantes).
7. Vérifiez que la règle de groupe de sécurité suivante existe :
 - Type : MySQL/Aurora
 - Plage de ports : 3306
 - Destination : `sg-1234567890example` / `rds-ec2-x`
 - Description : Règle pour autoriser les connexions à **database-tutorial** à partir de n'importe quelle instance à laquelle ce groupe de sécurité est attaché

8. Ouvrez la console Amazon RDS à l'adresse <https://console.aws.amazon.com/rds/>.
9. Dans la page de navigation, choisissez Databases (Bases de données).
10. Choisissez la base de données RDS que vous avez créée pour ce tutoriel.
11. Dans l'onglet Connectivity & security (Connectivité et sécurité), sous Security (Sécurité), VPC security groups (Groupes de sécurité VPC), vérifiez qu'un groupe de sécurité appelé **rds-ec2-x** est affiché.
12. Sélectionnez le groupe de sécurité **rds-ec2-x**. L'écran Security Groups (Groupes de sécurité) de la console EC2 s'ouvre.
13. Sélectionnez le groupe de sécurité **rds-ec2-x** pour l'ouvrir.
14. Choisissez l'onglet Inbound rules (Règles entrantes).
15. Vérifiez que la règle de groupe de sécurité suivante existe :
 - Type : MySQL/Aurora
 - Plage de ports : 3306
 - Source : **sg-0987654321example** / ec2-rds-x : il s'agit du groupe de sécurité qui est attribué à l'instance EC2 que vous avez vérifiée dans les étapes précédentes.
 - Description : Règle pour autoriser les connexions des instances EC2 avec **sg-1234567890example** attaché

En vérifiant que ces groupes de sécurité et ces règles de groupe de sécurité existent et qu'ils sont affectés à l'instance EC2 et à la base de données RDS comme décrit dans cette procédure, vous pouvez vérifier que la connexion a été automatiquement configurée en utilisant la fonction de connexion automatique.

Voir une animation : vérification de la configuration de la connexion



Vous avez terminé l'option 2 de ce tutoriel. Vous pouvez maintenant terminer l'option 3, qui vous apprend à configurer manuellement les groupes de sécurité qui ont été créés automatiquement dans l'option 2.

Option 3 : connexion manuelle de votre instance EC2 à votre base de données RDS en imitant la fonction de connexion automatique

Objectif

L'objectif de l'option 3 est d'apprendre à configurer manuellement la connexion entre une instance EC2 et une base de données RDS en reproduisant manuellement la configuration de la fonction de connexion automatique.

Avant de commencer

Vous aurez besoin des éléments suivants pour compléter ce tutoriel :

- Une instance EC2 qui se trouve dans le même VPC que la base de données RDS. Vous pouvez utiliser une instance EC2 existante ou suivre les étapes de la tâche 1 pour créer une nouvelle instance.
- Une base de données RDS qui se trouve dans le même VPC que l'instance EC2. Vous pouvez soit utiliser une base de données RDS existante, soit suivre les étapes de la tâche 2 pour créer une nouvelle base de données.
- Des autorisations pour appeler les opérations suivantes. Si vous avez terminé l'option 1 de ce tutoriel, vous disposez déjà de ces autorisations.
 - `ec2:AssociateRouteTable`
 - `ec2:AuthorizeSecurityGroupEgress`
 - `ec2:CreateRouteTable`
 - `ec2:CreateSecurityGroup`
 - `ec2:CreateSubnet`
 - `ec2:DescribeInstances`
 - `ec2:DescribeNetworkInterfaces`
 - `ec2:DescribeRouteTables`
 - `ec2:DescribeSecurityGroups`
 - `ec2:DescribeSubnets`
 - `ec2:ModifyNetworkInterfaceAttribute`
 - `ec2:RevokeSecurityGroupEgress`

Les tâches pour terminer l'option 3

- [Tâche 1 : lancement d'une instance EC2 – facultatif](#)
- [Tâche 2 : création d'une base de données RDS – facultatif](#)
- [Tâche 3 : connexion manuelle de votre instance EC2 à votre base de données RDS en créant des groupes de sécurité et en les affectant aux instances](#)

Tâche 1 : lancement d'une instance EC2 – facultatif

Note

Le lancement d'une instance n'est pas l'objet de ce tutoriel. Si vous disposez déjà d'une instance Amazon EC2 et que vous voulez l'utiliser dans ce tutoriel, vous pouvez ignorer cette tâche.

Objectif de la tâche

L'objectif de cette tâche est de lancer une instance EC2 afin que vous puissiez terminer la tâche 3 où vous configurez la connexion entre votre instance EC2 et votre base de données Amazon RDS.

Étapes pour lancer une instance EC2

Effectuez les étapes suivantes pour lancer une instance EC2 pour ce tutoriel.

Pour voir une animation de ces étapes, consultez [Voir une animation : lancement d'une instance EC2](#).

Configuration des instances EC2

Les étapes de cette tâche configurent l'instance EC2 comme suit :

- Nom de l'instance : **tutorial-instance**
- AMI : Amazon Linux 2
- Type d'instance : `t2.micro`
- Attribuer automatiquement l'adresse IP publique : Activé
- Groupe de sécurité avec les trois règles suivantes :
 - Autoriser SSH depuis votre adresse IP
 - Autoriser le trafic HTTPS depuis n'importe où
 - Autoriser le trafic HTTP depuis n'importe où

Important

Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

Pour lancer une instance EC2

1. [Connectez-vous à la console Amazon EC2 AWS Management Console et ouvrez-la à l'adresse `https://console.aws.amazon.com/ec2/`.](https://console.aws.amazon.com/ec2/)
2. Dans EC2 Dashboard (Tableau de bord EC2), choisissez Launch instance (Lancer l'instance).
3. Sous Name and tags (Noms et balises), pour Name (Nom), saisissez un nom pour identifier votre instance. Pour ce tutoriel, nommez l'instance **tutorial-instance-manual-1**. Bien que le nom de l'instance ne soit pas obligatoire, il vous aidera à l'identifier facilement.
4. Sous Application and OS Images (Images de l'application et du système d'exploitation), choisissez une AMI qui répond aux besoins de votre serveur Web. Ce tutoriel utilise Amazon Linux.
5. Sous Instance type (Type d'instance), pour Instance type (Type d'instance), sélectionnez un type d'instance qui répond aux besoins de votre serveur Web. Ce tutoriel utilise `t2.micro`.

Note

Vous pouvez utiliser Amazon EC2 dans le cadre du [niveau gratuit](#) à condition que votre AWS compte date de moins de 12 mois et que vous choisissiez un type d'`t2.microinstance` (ou `t3.micro` dans les régions où ce type d'instance n'`t2.micro`est pas disponible).

6. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez votre paire de clés.
7. Sous Network settings (Paramètres réseau), effectuez les opérations suivantes :
 - a. Pour Network (Réseau) et Subnet (Sous-réseau), si vous n'avez pas apporté de modifications à votre VPC ou à vos sous-réseaux par défaut, vous pouvez conserver les paramètres par défaut.

Si vous avez apporté des modifications à votre VPC ou à vos sous-réseaux par défaut, vérifiez ce qui suit :

- i. L'instance doit se trouver dans le même VPC que la base de données RDS. Par défaut, vous n'avez qu'un seul VPC.
- ii. Le VPC dans lequel vous lancez votre instance doit avoir une passerelle Internet qui lui est attachée afin que vous puissiez accéder à votre serveur Web depuis Internet. Votre VPC par défaut est automatiquement configuré avec une passerelle Internet.

- iii. Pour vous assurer que votre instance reçoit une adresse IP publique, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), vérifiez que Enable (Activer) est sélectionné. Si l'option Disable (Désactiver) est sélectionnée, choisissez Edit (Modifier) (à droite de Network Settings (Paramètres réseau)), puis, pour Auto-assign public IP (Attribuer automatiquement une adresse IP publique), choisissez Enable (Activer).
- b. Pour vous connecter à votre instance en utilisant SSH, vous avez besoin d'une règle de groupe de sécurité qui autorise le trafic SSH (Linux) ou RDP (Windows) à partir de l'adresse IPv4 publique de votre ordinateur. Par défaut, lorsque vous lancez une instance, un nouveau groupe de sécurité est créé avec une règle qui autorise le trafic SSH entrant de n'importe où.

Pour vous assurer que seule votre adresse IP peut se connecter à votre instance, sous Firewall (security groups) (Pare-feu (groupes de sécurité)), dans la liste déroulante située à côté de la case Allow SSH traffic from (Autoriser le trafic SSH depuis), choisissez My IP (Mon adresse IP).

- c. Pour autoriser le trafic depuis Internet vers votre instance, cochez les cases suivantes :
 - Allow HTTPs traffic from the internet (Autoriser le trafic HTTPs depuis Internet)
 - Allow HTTP traffic from the internet (Autoriser le trafic HTTP depuis Internet)
8. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance).
9. Sélectionnez View all instances (Afficher toutes les instances) pour fermer la page de confirmation et revenir à la console. Votre instance sera d'abord dans un état pending, puis passera à l'état running.

Si l'instance ne peut pas être lancée ou que l'état passe immédiatement à terminated au lieu de running, consultez [Résoudre les problèmes de lancement d'instance](#).

Pour plus d'informations sur le lancement d'une instance, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Voir une animation : lancement d'une instance EC2

The screenshot displays the Amazon EC2 console interface. On the left is a navigation sidebar with categories like EC2 Dashboard, Instances, Images, Elastic Block Store, and Network & Security. The main content area is divided into several sections:

- Resources:** A summary of EC2 resources in the Europe (Stockholm) Region.

Instances (running)	2	Dedicated Hosts	0	Elastic IPs	0
Instances	2	Key pairs	1	Load balancers	0
Placement groups	0	Security groups	10	Snapshots	1
Volumes	3				
- Launch instance:** A section with a "Launch instance" button and a "Migrate a server" link. Below it, a note states: "Your instances will launch in the Europe (Stockholm) Region".
- Scheduled events:** A section showing "No scheduled events" for the Europe (Stockholm) region.
- Service health:** A section showing the status of the service in the Europe (Stockholm) region as "This service is operating normally".
- Zones:** A table listing the available availability zones in the region.

Zone name	Zone ID
eu-north-1a	eun1-az1
eu-north-1b	eun1-az2
eu-north-1c	eun1-az3

Voici le moment pour [Tâche 2 : création d'une base de données RDS – facultatif](#).

Tâche 2 : création d'une base de données RDS – facultatif

Note

La création d'une base de données RDS n'est pas l'objet de cette partie du tutoriel. Si vous disposez déjà d'une base de données RDS et que vous voulez l'utiliser pour ce tutoriel, vous pouvez ignorer cette tâche.

Objectif de la tâche

L'objectif de cette tâche est de créer une base de données RDS. Vous utiliserez cette instance dans la tâche 3 lorsque vous la connecterez à votre instance EC2.

Étapes à suivre pour créer une base de données RDS

Suivez les étapes suivantes pour créer une base de données RDS pour l'option 3 de ce tutoriel.

Pour voir une animation de ces étapes, consultez [Voir une animation : création d'une instance de base de données](#).

Configuration de la base de données RDS

Les étapes de cette tâche configurent la base de données RDS comme suit :

- Type de moteur : MySQL
- Modèle : offre gratuite
- Identifiant d'instance de base de données : **tutorial-database-manual**
- Classe d'instance de base de données : `db.t3.micro`

Important

Dans un environnement de production, vous devez configurer votre instance pour répondre à vos besoins spécifiques.

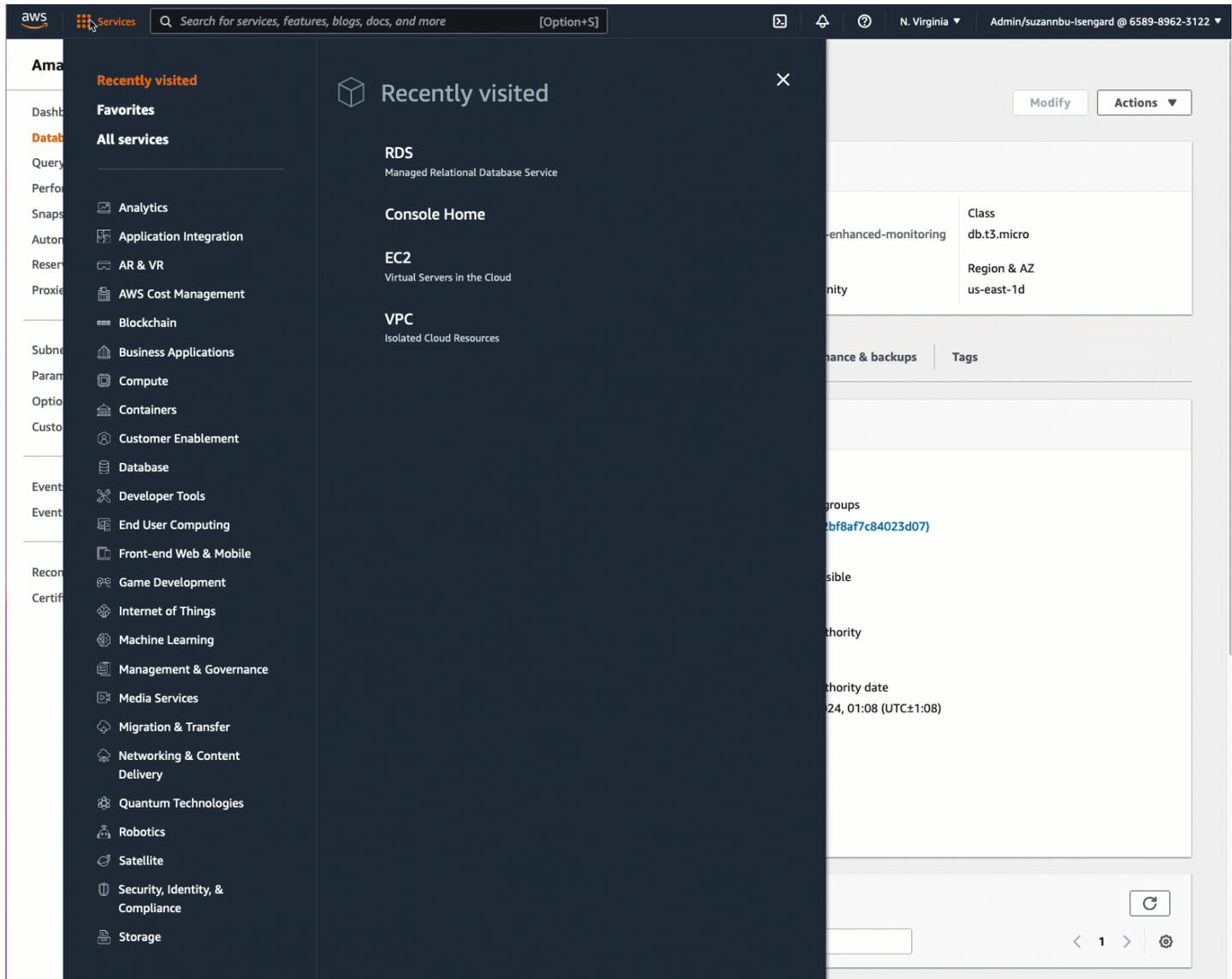
Pour créer une instance de base de données MySQL

1. Ouvrez la console Amazon RDS à l'adresse <https://console.aws.amazon.com/rds/>.
2. Dans le sélecteur de région (en haut à droite), choisissez l'instance Région AWS dans laquelle vous avez créé l'instance EC2. L'instance EC2 et l'instance de base de données doivent se trouver dans la même région.
3. Dans le tableau de bord, choisissez Create database (Créer une base de données).
4. Sous Choose a database creation method (Choisir une méthode de création de base de données), choisissez Easy create (Création facile). Lorsque vous choisissez cette option, la fonction de connexion automatique permettant de configurer automatiquement la connexion n'est pas disponible.
5. Sous Engine options (Options du moteur), pour Engine type (Type de moteur), choisissez MySQL.
6. Pour DB instance size (Taille de l'instance de base de données), choisissez Free tier (Offre gratuite).

7. Pour DB instance identifier (Identifiant d'instance de base de données), saisissez un nom pour la base de données RDS. Dans le cadre de ce didacticiel, entrez **tutorial-database-manual**.
8. Pour Master username (Nom d'utilisateur principal), laissez le nom par défaut, qui est **admin**.
9. Pour Master password (Mot de passe principal), saisissez un mot de passe dont vous pouvez vous souvenir pour ce tutoriel, puis, pour Confirm password (Confirmer le mot de passe), saisissez à nouveau le mot de passe.
10. Choisissez Créer une base de données.

Sur l'écran Databases (Bases de données), le Status (Statut) de la nouvelle instance de base de données est Creating (Création) jusqu'à ce que l'instance de base de données soit prête à être utilisée. Lorsque l'état passe à Available (Disponible), vous pouvez vous connecter à l'instance de base de données. En fonction de la quantité de stockage et de la classe d'instance de base de données, la mise à disposition de la nouvelle instance peut prendre jusqu'à 20 minutes.

Voir une animation : création d'une instance de base de données



Voici le moment pour [Tâche 3 : connexion manuelle de votre instance EC2 à votre base de données RDS en créant des groupes de sécurité et en les affectant aux instances.](#)

Tâche 3 : connexion manuelle de votre instance EC2 à votre base de données RDS en créant des groupes de sécurité et en les affectant aux instances

Objectif de la tâche

L'objectif de cette tâche est de reproduire la configuration de connexion de la fonction de connexion automatique en effectuant les opérations suivantes manuellement : vous créez deux nouveaux groupes de sécurité, puis vous ajoutez l'un à l'instance EC2 et l'autre à la base de données RDS.

Étapes pour créer de nouveaux groupes de sécurité et les ajouter aux instances

Effectuez les étapes suivantes pour connecter une instance EC2 à votre base de données RDS en créant deux nouveaux groupes de sécurité. Vous ajoutez ensuite un groupe de sécurité à l'instance EC2 et à la base de données RDS.

Pour créer deux nouveaux groupes de sécurité et en attribuer un à l'instance EC2 et l'autre à la base de données RDS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Créez d'abord le groupe de sécurité à ajouter à l'instance EC2, comme suit :
 - a. Dans le panneau de navigation, choisissez Groupes de sécurité.
 - b. Sélectionnez Create security group (Créer un groupe de sécurité).
 - c. Pour Security group name (Nom du groupe de sécurité), saisissez un nom descriptif pour le groupe de sécurité. Dans le cadre de ce didacticiel, entrez **ec2-rds-manual-configuration**.
 - d. Pour Description, saisissez une brève description. Dans le cadre de ce didacticiel, entrez **EC2 instance security group to allow EC2 instance to securely connect to RDS database**.
 - e. Sélectionnez Create security group (Créer un groupe de sécurité). Vous reviendrez à ce groupe de sécurité pour ajouter une règle sortante après avoir créé le groupe de sécurité de la base de données RDS.
3. Maintenant, créez le groupe de sécurité à ajouter à la base de données RDS, comme suit :
 - a. Dans le panneau de navigation, choisissez Groupes de sécurité.
 - b. Sélectionnez Create security group (Créer un groupe de sécurité).
 - c. Pour Security group name (Nom du groupe de sécurité), saisissez un nom descriptif pour le groupe de sécurité. Dans le cadre de ce didacticiel, entrez **rds-ec2-manual-configuration**.
 - d. Pour Description, saisissez une brève description. Dans le cadre de ce didacticiel, entrez **RDS database security group to allow EC2 instance to securely connect to RDS database**.
 - e. Sous Inbound rules (Règles entrantes), choisissez Add rule (Ajouter une règle), puis effectuez les opérations suivantes :
 - i. Pour Type, choisissez MySQL/Aurora.

- ii. Pour Source, choisissez le groupe de sécurité de l'instance EC2 `ec2-rds-manual-configuration` que vous avez créé à l'étape 2 de cette procédure.
 - f. Sélectionnez `Create security group` (Créer un groupe de sécurité).
4. Modifiez le groupe de sécurité de l'instance EC2 pour ajouter une règle sortante, comme suit :
 - a. Dans le panneau de navigation, choisissez `Groupes de sécurité`.
 - b. Sélectionnez le groupe de sécurité de l'instance EC2 (vous l'avez nommé **`ec2-rds-manual-configuration`**), puis choisissez l'onglet `Outbound rules` (Règles sortantes).
 - c. Choisissez `Edit outbound rules` (Modifier les règles sortantes).
 - d. Choisissez `Add rule` (Ajouter une règle) et effectuez les opérations suivantes :
 - i. Pour Type, choisissez `MySQL/Aurora`.
 - ii. Pour Source, choisissez le groupe de sécurité de la base de données RDS `rds-ec2-manual-configuration` que vous avez créé à l'étape 3 de cette procédure.
 - iii. Sélectionnez `Enregistrer les règles`.
5. Ajoutez le groupe de sécurité de l'instance EC2 à l'instance EC2 comme suit :
 - a. Dans le panneau de navigation, sélectionnez `Instances`.
 - b. Sélectionnez votre instance EC2, puis `Actions, Security (Sécurité), Change security groups` (Modifier les groupes de sécurité).
 - c. Sous `Associated security groups` (Groupes de sécurité associés), choisissez le champ `Select security groups` (Sélectionner les groupes de sécurité), choisissez `ec2-rds-manual-configuration` que vous avez créé précédemment, puis `Add security group` (Ajouter un groupe de sécurité).
 - d. Choisissez `Enregistrer`.
6. Ajoutez le groupe de sécurité de la base de données RDS à la base de données RDS comme suit :
 - a. Ouvrez la console Amazon RDS à l'adresse <https://console.aws.amazon.com/rds/>.
 - b. Dans le panneau de navigation, choisissez `Databases` (Bases de données) et sélectionnez votre base de données.
 - c. Sélectionnez `Modifier`.
 - d. Sous `Connectivity` (Connectivité), pour `Security group` (Groupe de sécurité), choisissez `rds-ec2-manual-configuration` que vous avez créé précédemment, puis cliquez sur `Continue` (Continuer).

- e. Sous Scheduling of Modifications (Planification des modifications), sélectionnez Apply immediately (Appliquer immédiatement).
- f. Choisissez Modifier l'instance de base de données.

Vous avez maintenant terminé les étapes manuelles qui imitent les étapes automatiques qui se produisent lorsque vous utilisez la fonction de connexion automatique.

Vous avez terminé l'option 3 de ce tutoriel. Si vous avez terminé les options 1, 2 et 3, et que vous n'avez plus besoin des ressources créées dans ce tutoriel, vous devriez les supprimer pour éviter d'encourir des coûts inutiles. Pour plus d'informations, consultez [Nettoyage](#).

Nettoyage

Maintenant que vous avez terminé le tutoriel, il est recommandé de nettoyer (supprimer) toutes les ressources que vous ne voulez plus utiliser. Le nettoyage AWS des ressources évite à votre compte d'encourir des frais supplémentaires.

Rubriques

- [Résiliation de votre instance EC2](#)
- [Suppression de votre base de données RDS](#)

Résiliation de votre instance EC2

Si vous avez lancé une instance EC2 spécifiquement pour ce tutoriel, vous pouvez la résilier pour ne plus encourir de frais associés.

Pour résilier une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance que vous avez créée pour ce tutoriel, puis choisissez Instance state (État de l'instance), Terminate instance (Résilier l'instance).
4. Choisissez Résilier lorsque vous êtes invité à confirmer.

Suppression de votre base de données RDS

Si vous avez créé une base de données RDS spécifiquement pour ce tutoriel, vous pouvez la supprimer pour ne plus encourir de frais associés.

Pour supprimer une base de données RDS à l'aide de la console

1. Ouvrez la console Amazon RDS à l'adresse <https://console.aws.amazon.com/rds/>.
2. Dans le panneau de navigation, choisissez Databases (Bases de données).
3. Sélectionnez la base de données RDS que vous avez créée pour ce tutoriel, puis choisissez Actions, Delete (Supprimer).
4. Saisissez **delete me** dans la case, puis choisissez Delete (Supprimer).

Identifiez vos instances EC2

Vous devrez peut-être déterminer si votre application s'exécute sur une instance EC2, en particulier si vous disposez d'un environnement informatique mixte. Chaque instance possède un document d'identité d'instance signé que vous pouvez vérifier de manière cryptographique. Vous pouvez trouver ces documents à l'adresse locale non routable suivante. <http://169.254.169.254/latest/dynamic/instance-identity/> Pour plus d'informations, consultez [Documents d'identité d'instance](#).

Inspecter l'UUID du système

Vous pouvez obtenir l'UUID du système et rechercher dans le premier octet de l'UUID EC2 (sous Linux, cela peut être en minuscules). `ec2` Cette méthode est rapide, mais potentiellement imprécise, car il est peu probable qu'un système autre qu'une instance EC2 possède un UUID commençant par ces caractères. De plus, certaines versions de SMBIOS utilisent le format little-endian, qui n'est pas inclus EC2 au début de l'UUID. Cela peut être le cas pour les instances EC2 qui utilisent SMBIOS 2.4 pour Windows, ou pour les distributions Linux autres qu'Amazon Linux 2 qui ont leur propre implémentation de SMBIOS.

Exemple Linux : obtenir l'UUID depuis DMI (AMI HVM uniquement)

Utilisez la commande suivante pour obtenir l'UUID à l'aide de DMI (Desktop Management Interface) :

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

Dans l'exemple de sortie suivant, l'UUID commence par « EC2 », ce qui indique que le système est probablement une instance EC2.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

Dans l'exemple de sortie qui suit, l'UUID est représenté au format Little Endian :

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Sinon, pour les instances construites sur le système Nitro, vous pouvez utiliser la commande suivante :

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Si la sortie est un ID d'instance, comme l'exemple de sortie suivant, le système est une instance EC2 :

```
i-0af01c0123456789a
```

Exemple Linux : obtenir l'UUID depuis l'hyperviseur (AMI PV uniquement)

Utilisez la commande suivante pour obtenir l'UUID de l'hyperviseur :

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

Dans l'exemple de sortie suivant, l'UUID commence par « ec2 », ce qui indique que le système est probablement une instance EC2.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Exemple Windows : obtenir l'UUID à l'aide de WMI ou de Windows PowerShell

Utilisez l'utilitaire de ligne de commande Windows Management Instrumentation Command Line (WMIC) comme suit :

```
wmic path win32_computersystemproduct get uuid
```

Si vous utilisez Windows PowerShell, vous pouvez également utiliser l'Get-WmiObjectapplet de commande comme suit :

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select  
UUID
```

Dans l'exemple de sortie suivant, l'UUID commence par « EC2 », ce qui indique que le système est probablement une instance EC2.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Pour les instances utilisant SMBIOS 2.4, l'UUID peut être représenté au format Little Endian. Par exemple :

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Inspecter l'identificateur de génération de machine virtuelle du système

Un identificateur de génération de machine virtuelle consiste en un tampon unique de 128 bits interprété comme un entier unique aléatoire cryptographique. Vous pouvez récupérer l'identificateur de génération de machine virtuelle pour identifier votre instance Amazon Elastic Compute Cloud. L'identificateur de génération est exposé dans le système d'exploitation invité de l'instance via une entrée de table ACPI. La valeur change si votre machine est clonée, copiée ou importée dans AWS, par exemple avec [VM Import/Export](#).

Exemple : récupérer l'identifiant de génération de machine virtuelle depuis Linux

Vous pouvez utiliser les commandes suivantes pour récupérer l'identifiant de génération de machine virtuelle à partir de vos instances exécutant Linux.

Amazon Linux 2

1. Mettez à jour vos packages logiciels existants, le cas échéant, à l'aide de la commande suivante :

```
sudo yum update
```

2. Si nécessaire, créez le package busybox à l'aide de la commande suivante :

```
sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
```

3. Si nécessaire, installez les packages préalables à l'aide de la commande suivante :

```
sudo yum install busybox.rpm iasl -y
```

4. Exécutez la commande `iasl` suivante pour produire une sortie à partir de la table ACPI :

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

5. Exécutez la commande suivante pour vérifier la sortie de la commande `iasl` :

```
cat SSDT2.dsl
```

La sortie doit fournir l'espace d'adressage requis pour récupérer l'identificateur de génération de machine virtuelle :

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
```

```

*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*   Signature       "SSDT"
*   Length          0x0000007B (123)
*   Revision        0x01
*   Checksum        0xB8
*   OEM ID          "AMAZON"
*   OEM Table ID    "AMZNSSDT"
*   OEM Revision    0x00000001 (1)
*   Compiler ID     "AMZN"
*   Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
  Scope (\_SB)
  {
    Device (VMGN)
    {
      Name (_CID, "VM_Gen_Counter") // _CID: Compatible ID
      Name (_DDN, "VM_Gen_Counter") // _DDN: DOS Device Name
      Name (_HID, "AMZN0000") // _HID: Hardware ID
      Name (ADDR, Package (0x02)
      {
        0xFED01000,
        Zero
      })
    }
  }
}

```

- (Facultatif) Augmentez les autorisations de votre terminal pour les étapes restantes à l'aide de la commande suivante :

```
sudo -s
```

- Utilisez la commande suivante pour stocker l'espace d'adressage précédemment collecté :

```
VMGN_ADDR=0xFED01000
```

- Utilisez la commande suivante pour parcourir l'espace d'adressage et créer l'identificateur de génération de machine virtuelle :

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $((VMGN_ADDR + $offset)) | sed 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Récupérez l'identificateur de génération de machine virtuelle à partir du fichier de sortie à l'aide de la commande suivante :

```
cat vmgenid ; echo
```

Votre sortie doit ressembler à ce qui suit :

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Mettez à jour vos packages logiciels existants, le cas échéant, à l'aide de la commande suivante :

```
sudo apt update
```

2. Si nécessaire, installez les packages préalables à l'aide de la commande suivante :

```
sudo apt install busybox iasl -y
```

3. Exécutez la commande `iasl` suivante pour produire une sortie à partir de la table ACPI :

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Exécutez la commande suivante pour vérifier la sortie de la commande `iasl` :

```
cat SSDT2.dsl
```

La sortie doit fournir l'espace d'adressage requis pour récupérer l'identificateur de génération de machine virtuelle :

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation
```

```

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*   Signature          "SSDT"
*   Length             0x0000007B (123)
*   Revision           0x01
*   Checksum           0xB8
*   OEM ID             "AMAZON"
*   OEM Table ID       "AMZNSSDT"
*   OEM Revision       0x00000001 (1)
*   Compiler ID        "AMZN"
*   Compiler Version   0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
  Scope (\_SB)
  {
    Device (VMGN)
    {
      Name (_CID, "VM_Gen_Counter") // _CID: Compatible ID
      Name (_DDN, "VM_Gen_Counter") // _DDN: DOS Device Name
      Name (_HID, "AMZN0000") // _HID: Hardware ID
      Name (ADDR, Package (0x02)
      {

```

```
        0xFED01000,  
        Zero  
    })  
}  
}  
}
```

- (Facultatif) Augmentez les autorisations de votre terminal pour les étapes restantes à l'aide de la commande suivante :

```
sudo -s
```

- Utilisez les commandes suivantes pour stocker l'espace d'adressage précédemment collecté :

```
VMGN_ADDR=0xFED01000
```

- Utilisez la commande suivante pour parcourir l'espace d'adressage et créer l'identificateur de génération de machine virtuelle :

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $((VMGN_ADDR + $offset)) | sed  
's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

- Récupérez l'identificateur de génération de machine virtuelle à partir du fichier de sortie à l'aide de la commande suivante :

```
cat vmgenid ; echo
```

Votre sortie doit ressembler à ce qui suit :

```
EC2F335D979132C4165896753E72BD1C
```

Exemple : récupérer l'identifiant de génération de machine virtuelle depuis Windows

Vous pouvez créer un exemple d'application pour récupérer l'identificateur de génération de machine virtuelle à partir de vos instances exécutant Windows. Pour plus d'informations, consultez [Obtention de l'identificateur de génération de l'ordinateur virtuel](#) dans la documentation Microsoft.

Gérez les paramètres système de votre instance Amazon EC2

Après avoir lancé votre instance, vous pouvez vous connecter en tant qu'administrateur pour apporter des modifications. Cette section est consacrée à la gestion des paramètres système de votre instance.

Table des matières

- [Définissez l'heure pour votre instance Amazon EC2](#)
- [Contrôle de l'état du processeur pour votre instance Linux Amazon EC2](#)
- [Optimiser les options d'UC](#)
- [AMD SEV-SNP sur Amazon EC2](#)
- [Ajouter des composants du système Windows à l'aide du support d'installation](#)
- [Gérez les utilisateurs du système sur votre instance Linux](#)
- [Définissez le mot de passe d'administrateur Windows pour votre instance](#)

Définissez l'heure pour votre instance Amazon EC2

Une référence temporelle cohérente et précise sur votre instance Amazon EC2 est essentielle pour de nombreuses tâches et processus de serveur. Les horodatages dans les journaux système jouent un rôle essentiel pour identifier le moment où les problèmes sont survenus et l'ordre chronologique des événements. Lorsque vous utilisez le AWS CLI ou un AWS SDK pour effectuer des demandes depuis votre instance, ces outils signent les demandes en votre nom. Si les paramètres de date et d'heure de votre instance sont inexacts, cela peut entraîner un écart entre la date figurant dans la signature et la date de la demande, ce qui peut entraîner le AWS rejet de vos demandes.

Pour répondre à cet aspect important, le Service de synchronisation temporelle d'Amazon, qui est accessible à partir de toutes les instances EC2 et est utilisé par plusieurs Services AWS. Le service utilise une flotte d'horloges de référence atomiques et connectées par satellite Région AWS pour fournir des relevés horaires précis et actuels conformément à la norme mondiale UTC (temps universel coordonné).

Le Service de synchronisation temporelle d'Amazon utilise le protocole NTP (Network Time Protocol) ou fournit une horloge matérielle PTP (Precision Time Protocol) locale sur les [instances prises en charge](#). L'horloge matérielle PTP prend en charge le protocole NTP ou une connexion PTP directe. Les connexions NTP et PTP directes utilisent la même source de temps très précise, mais la connexion PTP directe est plus précise que la connexion NTP. La connexion NTP au service Service

de synchronisation temporelle d'Amazon en charge la correction des secondes intercalaires, tandis que la connexion PTP à l'horloge matérielle PTP ne corrige pas le temps. Pour plus d'informations, consultez [Secondes intercalaires](#).

Pour de meilleures performances, nous vous recommandons d'utiliser le service Amazon Time Sync local sur vos instances EC2. Pour effectuer une sauvegarde vers le service Amazon Time Sync local sur vos instances et pour connecter des ressources extérieures à Amazon EC2 au service Amazon Time Sync, vous pouvez utiliser le service public Amazon Time Sync situé à l'adresse `time.aws.com`. Le Service de synchronisation temporelle d'Amazon public, comme le Service de synchronisation temporelle d'Amazon local, corrige automatiquement les secondes intercalaires qui sont ajoutées au temps UTC. Le service public Amazon Time Sync est pris en charge dans le monde entier par notre flotte d'horloges de référence atomiques et connectées par satellite dans chacun d'entre eux. Région AWS

Rubriques

- [Configuration de votre instance pour qu'elle utilise le Service de synchronisation temporelle d'Amazon local](#)
- [Configuration de votre instance ou de tout appareil connecté à Internet pour qu'il utilise le Service de synchronisation temporelle d'Amazon public](#)
- [Comparez les horodatages de vos instances Linux](#)
- [Modifier le fuseau horaire de votre instance](#)
- [Secondes intercalaires](#)
- [Ressources connexes](#)

Configuration de votre instance pour qu'elle utilise le Service de synchronisation temporelle d'Amazon local

Vos instances peuvent accéder au Service de synchronisation temporelle d'Amazon local comme suit :

- Via le protocole NTP sur les points de terminaison d'adresses IP suivants :
 - IPv4 : 169.254.169.123
 - IPv6 : fd00:ec2::123 (Accessible uniquement par [les instances créées sur le système AWS Nitro](#).)
- (Linux uniquement) Via une connexion PTP directe pour se connecter à une horloge matérielle PTP locale :

- PHC0

Les AMI Amazon Linux, les AMI Windows et la plupart des AMI partenaires configurent votre instance pour utiliser le point de terminaison IPv4 NTP par défaut. Il s'agit du paramètre recommandé pour la plupart des charges de travail des clients. Aucune autre configuration n'est requise pour les instances lancées à partir de ces AMI, sauf si vous souhaitez utiliser le point de terminaison IPv6 ou vous connecter directement à l'horloge matérielle PTP.

Les connexions NTP et PTP ne nécessitent aucune modification de configuration VPC et votre instance n'a pas besoin d'accéder à Internet.

Note

Seules les instances Linux peuvent utiliser une connexion PTP directe pour se connecter à l'horloge matérielle PTP locale. Les instances Windows utilisent le protocole NTP pour se connecter à l'horloge matérielle PTP locale.

Rubriques

- [Connexion au point de terminaison IPv4 du Service de synchronisation temporelle d'Amazon](#)
- [Connexion au point de terminaison IPv6 du Service de synchronisation temporelle d'Amazon](#)
- [Connexion à l'horloge matérielle PTP](#)

Connexion au point de terminaison IPv4 du Service de synchronisation temporelle d'Amazon

Cette section décrit comment configurer votre instance pour qu'elle utilise le Service de synchronisation temporelle d'Amazon local via le point de terminaison IPv4.

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Linux

AL2023 et les dernières versions des AMI Amazon Linux 2 et Amazon Linux sont configurées pour utiliser le point de terminaison IPv4 du Service de synchronisation temporelle d'Amazon par défaut. Aucune autre configuration n'est requise pour les instances lancées à partir de ces AMI et vous pouvez ignorer la procédure suivante.

Si vous utilisez une AMI sur laquelle le Service de synchronisation temporelle d'Amazon n'est pas configuré par défaut, utilisez l'une des procédures suivantes pour configurer le Service de synchronisation temporelle d'Amazon sur votre instance à l'aide du client `chrony`. Cela nécessite d'ajouter une entrée de serveur pour le Service de synchronisation temporelle d'Amazon au fichier de configuration `chrony`.

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Amazon Linux

Pour vous connecter au point de terminaison IPv4 du Service de synchronisation temporelle d'Amazon sur Amazon Linux à l'aide de `chrony`

1. Connectez-vous à votre instance et désinstallez le service NTP.

```
[ec2-user ~]$ sudo yum erase 'ntp*
```

2. Installez le package `chrony`.

```
[ec2-user ~]$ sudo yum install chrony
```

3. Ouvrez le fichier `/etc/chrony.conf` avec un éditeur de texte (tel que `vim` ou `nano`). Vérifiez que le fichier contienne la ligne suivante :

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

Si la ligne est présente, alors le Service de synchronisation temporelle d'Amazon est déjà configuré pour utiliser le point de terminaison IPv4 du Service de synchronisation temporelle d'Amazon et vous pouvez passer à l'étape suivante. Si ce n'est pas le cas, ajoutez la ligne après toute autre instruction `server` ou `pool` déjà présente dans le fichier, puis enregistrer les changements.

4. Relancez le démon `chrony` (`chronyd`).

```
[ec2-user ~]$ sudo service chronyd restart
```

```
Starting chronyd: [ OK ]
```

Note

Sur RHEL ou CentOS (jusqu'à la version 6), le nom du service est `chrony` au lieu de `chronyd`.

- Pour configurer `chronyd` afin de lancer ce service à chaque démarrage système, utilisez la commande `chkconfig`.

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

- Vérifiez que `chrony` utilise le point de terminaison IPv4 `169.254.169.123` pour synchroniser le temps.

```
[ec2-user ~]$ chronyc sources -v
```

```
210 Number of sources = 7

    .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
    /  .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
    | /  '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
    ||                                     .- xxxx [ yyyy ] +/-
zzzz
    ||      Reachability register (octal) -.      |  xxxx = adjusted
offset,
    ||      Log2(Polling interval) --.      |      |  yyyy = measured
offset,
    ||                                     \      |      |  zzzz = estimated
error.
    ||                                     |      |      \
    MS Name/IP address          Stratum Poll Reach LastRx Last sample
=====
    ^* 169.254.169.123           3   6   17   43   -30us[ -226us] +/-
287us
    ^- ec2-12-34-231-12.eu-west> 2   6   17   43   -388us[ -388us] +/-
11ms
```

```

^* tshirt.heanet.ie          1  6  17  44  +178us[ +25us] +/-
1959us
^? tbag.heanet.ie           0  6   0  -   +0ns[ +0ns] +/-
0ns
^? bray.walcz.net           0  6   0  -   +0ns[ +0ns] +/-
0ns
^? 2a05:d018:c43:e312:ce77:> 0  6   0  -   +0ns[ +0ns] +/-
0ns
^? 2a05:d018:dab:2701:b70:b> 0  6   0  -   +0ns[ +0ns] +/-
0ns

```

Dans le résultat retourné, ^* indique la source de temps préférée.

7. Vérifiez les métriques de synchronisation du temps présentées par chrony.

```
[ec2-user ~]$ chronyc tracking
```

```

Reference ID      : A9FEA97B (169.254.169.123)
Stratum          : 4
Ref time (UTC)   : Wed Nov 22 13:18:34 2017
System time      : 0.000000626 seconds slow of NTP time
Last offset      : +0.002852759 seconds
RMS offset       : 0.002852759 seconds
Frequency        : 1.187 ppm fast
Residual freq    : +0.020 ppm
Skew             : 24.388 ppm
Root delay       : 0.000504752 seconds
Root dispersion  : 0.001112565 seconds
Update interval  : 64.4 seconds
Leap status      : Normal

```

Ubuntu

Pour vous connecter au point de terminaison IPv4 du Service de synchronisation temporelle d'Amazon sur Ubuntu à l'aide de chrony

1. Connectez-vous à votre instance et utilisez apt pour installer le package chrony.

```
ubuntu:~$ sudo apt install chrony
```

Note

Si nécessaire, mettez d'abord à jour votre instance en exécutant `sudo apt update`.

- Ouvrez le fichier `/etc/chrony/chrony.conf` avec un éditeur de texte (tel que vim ou nano). Ajoutez la ligne suivante avant toute autre instruction `server` ou `pool` déjà présente dans le fichier, puis enregistrez les changements :

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

- Redémarrez le service chrony.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

- Vérifiez que chrony utilise le point de terminaison IPv4 `169.254.169.123` pour synchroniser le temps.

```
ubuntu:~$ chronyc sources -v
```

```
210 Number of sources = 7

      .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
      /.- Source state '*' = current synced, '+' = combined , '-' = not
combined,
| /  '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
||                                     .- xxxx [ yyyy ]
+/- zzzz
||      Reachability register (octal) -.      | xxxx =
adjusted offset,
||      Log2(Polling interval) --.      |      | yyyy =
measured offset,
||                                     \      |      | zzzz =
estimated error.
||                                     |      |      \
MS Name/IP address          Stratum Poll Reach LastRx Last sample
```

```

=====
^* 169.254.169.123          3  6  17  12  +15us[ +57us]
+/- 320us
^- tbag.heanet.ie         1  6  17  13 -3488us[-3446us]
+/- 1779us
^- ec2-12-34-231-12.eu-west- 2  6  17  13 +893us[ +935us]
+/- 7710us
^? 2a05:d018:c43:e312:ce77:6 0  6  0  10y +0ns[ +0ns]
+/- 0ns
^? 2a05:d018:d34:9000:d8c6:5 0  6  0  10y +0ns[ +0ns]
+/- 0ns
^? tshirt.heanet.ie       0  6  0  10y +0ns[ +0ns]
+/- 0ns
^? bray.walcz.net        0  6  0  10y +0ns[ +0ns]
+/- 0ns

```

Dans le résultat retourné, sur la ligne commençant par `^*`, cela indique la source de temps préférée.

- Vérifiez les métriques de synchronisation du temps présentées par `chrony`.

```
ubuntu:~$ chronyc tracking
```

```

Reference ID      : 169.254.169.123 (169.254.169.123)
Stratum          : 4
Ref time (UTC)   : Wed Nov 29 07:41:57 2017
System time      : 0.000000011 seconds slow of NTP time
Last offset      : +0.000041659 seconds
RMS offset       : 0.000041659 seconds
Frequency        : 10.141 ppm slow
Residual freq    : +7.557 ppm
Skew             : 2.329 ppm
Root delay       : 0.000544 seconds
Root dispersion  : 0.000631 seconds
Update interval  : 2.0 seconds
Leap status      : Normal

```

SUSE Linux

À partir de SUSE Linux Enterprise Server 15, `chrony` est l'implémentation par défaut de NTP.

Pour vous connecter au point de terminaison IPv4 du Service de synchronisation temporelle d'Amazon sur SUSE Linux à l'aide de chrony

1. Ouvrez le fichier `/etc/chrony.conf` avec un éditeur de texte (tel que vim ou nano).
2. Vérifiez que le fichier contient la ligne suivante :

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

Si la ligne n'est pas présente, vous pouvez l'ajouter manuellement.

3. Placez en commentaire les autres lignes sur le serveur ou le groupe (pool).
4. Ouvrez yaST et activez le service chrony.

Windows

Depuis la version d'août 2018, les AMI Windows utilisent Amazon Time Sync Service par défaut. Aucune autre configuration n'est requise pour les instances lancées à partir de ces AMI et vous pouvez ignorer les procédures suivantes.

Si vous utilisez une AMI sur laquelle le service Amazon Time Sync n'est pas configuré par défaut, vérifiez d'abord votre configuration NTP actuelle. Si votre instance utilise déjà le point de terminaison IPv4 du Service de synchronisation temporelle d'Amazon, aucune autre configuration n'est requise. Si votre instance n'utilise pas le Service de synchronisation temporelle d'Amazon, suivez la procédure pour modifier le serveur NTP afin qu'il utilise le Service de synchronisation temporelle d'Amazon.

Pour vérifier la configuration NTP

1. Depuis votre instance, ouvrez une fenêtre d'invite de commande.
2. Obtenez la configuration NTP actuelle en tapant la commande suivante :

```
w32tm /query /configuration
```

Cette commande renvoie les paramètres de configuration actuels de l'instance Windows et indique si vous êtes connecté au Service de synchronisation temporelle d'Amazon.

3. (Facultatif) Obtenez l'état de la configuration actuelle en tapant la commande suivante :

```
w32tm /query /status
```

Cette commande renvoie des informations comme la dernière fois que l'instance s'est synchronisée sur le serveur NTP et l'intervalle d'interrogation.

Pour modifier le serveur NTP pour utiliser Amazon Time Sync Service

1. A partir d'une fenêtre d'invite de commande, exécutez la commande suivante :

```
w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
```

2. Vérifiez vos nouveaux paramètres en exécutant la commande suivante :

```
w32tm /query /configuration
```

Dans la sortie retournée, vérifiez que `NtpServer` affiche le point de terminaison IPv4 `169.254.169.123`.

Paramètres du protocole NTP (Network Time Protocol) par défaut pour les AMI Windows Amazon

Amazon Machine Images (AMI) respecte généralement les out-of-the-box valeurs par défaut, sauf dans les cas où des modifications sont nécessaires pour fonctionner sur l'infrastructure EC2. Les paramètres suivants ont été déterminés comme étant efficaces dans un environnement virtuel et permettant de maintenir la dérive d'horloge dans une précision d'une seconde :

- Intervalle de mise à jour — Détermine la fréquence à laquelle le service horaire ajustera l'heure du système pour qu'elle soit précise. AWS configure l'intervalle de mise à jour pour qu'il se produise une fois toutes les deux minutes.
- Serveur NTP – Depuis la version d'août 2018, les AMI utilisent le Service de synchronisation temporelle d'Amazon par défaut. Cette fois, le service est accessible depuis n'importe quel point de Région AWS terminaison IPv4 `169.254.169.123`. De plus, l'indicateur `0x9` indique que le service temporel agit en tant que client et qu'il convient d'utiliser `SpecialPollInterval` pour déterminer la fréquence à laquelle se signaler auprès du serveur horaire configuré.
- Type – « NTP » signifie que le service agira comme client NTP autonome et non pas dans le cadre d'un domaine.
- Activé et `InputProvider` — Le service horaire est activé et fournit du temps au système d'exploitation.

- Intervalle d'interrogation spécial — Vérifie par rapport au serveur NTP configuré toutes les 900 secondes (15 minutes).

Chemin de registre	Nom de la touche	Données
HKLM:\System \ CurrentControl Set \ services \ w32time \ Config	UpdateInterval	120
HKLM:\System \ CurrentControl Set \ services \ w32time \ Parameters	NtpServer	169.254.169.123,0x9
HKLM:\System \ CurrentControl Set \ services \ w32time \ Parameters	Type	NTP
HKLM:\System \ CurrentControl Set \ services \ w32time \ \ TimeProviders NtpClient	Activées	1
HKLM:\System \ CurrentControl Set \ services \ w32time \ \ TimeProviders NtpClient	InputProvider	1
HKLM:\System \ CurrentControl Set \ services \ w32time \ \ TimeProviders NtpClient	SpecialPollInterval	900

Connexion au point de terminaison IPv6 du Service de synchronisation temporelle d'Amazon

Cette section présente les différences avec les étapes décrites dans [Connexion au point de terminaison IPv4 du Service de synchronisation temporelle d'Amazon](#) si vous configurez votre instance pour qu'elle utilise le Service de synchronisation temporelle d'Amazon local via le point de

terminaison IPv6. Il n'explique pas l'intégralité du processus de configuration Amazon Time Sync Service.

Le point de terminaison IPv6 n'est accessible que sur [les instances créées sur le système AWS Nitro](#).

Note

Nous ne recommandons pas d'utiliser à la fois les entrées de point de terminaison IPv4 et IPv6. Les paquets NTP IPv4 et IPv6 proviennent du même serveur local pour votre instance. La configuration des points de terminaison IPv4 et IPv6 n'est pas nécessaire et n'améliorera pas la précision de l'heure sur votre instance.

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Linux

Selon la distribution Linux que vous utilisez, lorsque vous atteindrez l'étape de modification du fichier `chrony.conf`, vous utiliserez le point de terminaison IPv6 du service Amazon Time Sync (`fd00:ec2::123`) plutôt que le point de terminaison IPv4 (`() : 169.254.169.123`) :

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Enregistrez le fichier et vérifiez que `chrony` utilise le point de terminaison IPv6 `fd00:ec2::123` pour synchroniser le temps :

```
[ec2-user ~]$ chronyc sources -v
```

Dans la sortie, si vous voyez le point de terminaison IPv6 `fd00:ec2::123`, la configuration est terminée.

Windows

Lorsque vous atteindrez l'étape consistant à modifier le serveur NTP pour utiliser le service Amazon Time Sync, vous utiliserez le point de terminaison IPv6 du service Amazon Time Sync (`fd00:ec2::123`) plutôt que le point de terminaison IPv4 (`169.254.169.123`) :

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Vérifiez que vos nouveaux paramètres utilisent le point de terminaison `fd00:ec2::123 IPv6` pour synchroniser l'heure :

```
w32tm /query /configuration
```

Dans le résultat, vérifiez que le point de terminaison `fd00:ec2::123 IPv6` est `NtpServer` affiché.

Connexion à l'horloge matérielle PTP

L'horloge matérielle PTP fait partie du [AWS système Nitro](#). Elle est donc directement accessible sur les [instances EC2 virtualisées et matériel nu prises en charge](#) sans utiliser les ressources du client.

Les points de terminaison NTP de l'horloge matérielle PTP sont les mêmes que ceux de la connexion du Service de synchronisation temporelle d'Amazon normale via IPv4 ou IPv6. Si votre logiciel est configuré pour le point de terminaison NTP et s'exécute sur une instance dotée d'une horloge matérielle PTP, il sera automatiquement connecté à l'horloge matérielle PTP via NTP.

Prérequis

L'horloge matérielle PTP est disponible sur une instance lorsque les conditions suivantes sont remplies :

- Soutenu Régions AWS : USA Est (Virginie du Nord) et Asie-Pacifique (Tokyo)
- Familles d'instances prises en charge
 - Usage général : M7a, M7g, M7gD, M7i
 - Optimisé pour le calcul : C7a, C7gd, C7i
 - Mémoire optimisée : R7a, R7g, R7gd, R7i
- (Linux uniquement) Le pilote ENA version 2.10.0 ou ultérieure est installé sur un système d'exploitation pris en charge. Pour plus d'informations sur les systèmes d'exploitation pris en charge, consultez les [conditions requises pour les pilotes](#) sur GitHub.

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Linux

Cette section décrit comment configurer votre instance pour qu'elle utilise le Service de synchronisation temporelle d'Amazon local via l'horloge matérielle PTP à l'aide d'une connexion PTP

directe. Cela nécessite l'ajout d'une entrée de serveur pour l'horloge matérielle PTP dans le fichier de configuration `chrony`.

Si votre instance possède une horloge matérielle PTP et que vous avez configuré la connexion NTP (vers le point de terminaison IPv4 ou IPv6), l'heure de votre instance est automatiquement calculée à partir de l'horloge matérielle PTP. Les étapes ci-dessous permettent de configurer la connexion PTP directe, qui vous donnera une heure plus précise que la connexion NTP.

Pour vous connecter à l'horloge matérielle PTP

1. Connectez-vous à votre instance et installez le pilote de noyau Linux pour l'Adaptateur réseau élastique (ENA) version 2.10.0 ou ultérieure. Pour les instructions d'installation, consultez le [pilote de noyau Linux pour la famille Elastic Network Adapter \(ENA\)](#) sur GitHub.
2. Vérifiez que l'appareil `/dev/ptp0` apparaît sur votre instance.

```
[ec2-user ~]$ ls /dev/ptp0
```

La sortie attendue est la suivante : Si `/dev/ptp0` ce n'est pas dans la sortie, le pilote ENA n'a pas été correctement installé. Passez en revue l'étape 1 de cette procédure pour installer le pilote.

```
/dev/ptp0
```

3. Modifiez `/etc/chrony.conf` à l'aide d'un éditeur de texte et ajoutez la ligne suivante n'importe où dans le fichier.

```
refclock PHC /dev/ptp0 poll 0 delay 0.000010 prefer
```

4. Redémarrez `chrony` à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo systemctl restart chronyd
```

5. Vérifiez que `chrony` utilise l'horloge matérielle PTP pour synchroniser l'heure sur cette instance.

```
[ec2-user ~]$ chronyc sources
```

Sortie attendue

```
MS Name/IP address          Stratum Poll Reach LastRx Last sample
```

```
=====
#* PHC0                0  0  377  1  +2ns[ +1ns] +/-  5031ns
```

Dans le résultat retourné, * indique la source de temps préférée. PHC0 correspond à l'horloge matérielle PTP. Vous devrez peut-être attendre quelques secondes après avoir redémarré chrony pour que l'astérisque apparaisse.

Windows

Les instances Windows ne prennent en charge qu'une connexion NTP à l'horloge matérielle PTP locale.

Les points de terminaison NTP de l'horloge matérielle PTP sont les mêmes que ceux de la connexion du Service de synchronisation temporelle d'Amazon normale via IPv4 ou IPv6. Si votre logiciel est configuré pour se connecter à un point de terminaison NTP et s'exécute sur une instance dotée d'une horloge matérielle PTP, il sera automatiquement connecté à l'horloge matérielle PTP via NTP.

Configuration de votre instance ou de tout appareil connecté à Internet pour qu'il utilise le Service de synchronisation temporelle d'Amazon public

Vous pouvez configurer votre instance, ou tout appareil connecté à Internet tel que votre ordinateur local ou un serveur sur site, pour utiliser le Service de synchronisation temporelle d'Amazon public, accessible via Internet à l'adresse `time.aws.com`. Vous pouvez utiliser le service public Amazon Time Sync comme solution de sauvegarde pour le service Amazon Time Sync local et pour connecter des ressources extérieures AWS au service Amazon Time Sync.

Note

Pour de meilleures performances, nous vous recommandons d'utiliser le service Amazon Time Sync local sur vos instances et de n'utiliser que le service public Amazon Time Sync en tant que sauvegarde.

Suivez les instructions relatives au système d'exploitation de votre instance ou de votre appareil.

Linux

Pour configurer votre instance ou appareil Linux afin qu'il utilise le Service de synchronisation temporelle d'Amazon public à l'aide de `chrony` ou `ntpd`

1. Modifiez `/etc/chrony.conf` (si vous utilisez `chrony`) ou `/etc/ntp.conf` (si vous utilisez `ntpd`) à l'aide d'un éditeur de texte comme suit :
 - a. Pour empêcher votre instance ou votre appareil d'essayer de mélanger des serveurs corrigés et non corrigés, supprimez ou commentez les lignes commençant par `server` sauf les connexions existantes au Service de synchronisation temporelle d'Amazon local.

Important

Si vous configurez votre instance EC2 pour qu'elle se connecte au Service de synchronisation temporelle d'Amazon public, ne supprimez pas la ligne suivante qui définit votre instance pour qu'elle se connecte au Service de synchronisation temporelle d'Amazon local. Le Service de synchronisation temporelle d'Amazon local fournit une connexion plus directe et une meilleure précision de l'horloge. Le Service de synchronisation temporelle d'Amazon public doit uniquement être utilisé comme sauvegarde.

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

- b. Ajoutez la ligne suivante pour vous connecter au Service de synchronisation temporelle d'Amazon public.

```
pool time.aws.com iburst
```

2. Redémarrez le démon à l'aide de l'une des commandes suivantes.

- `chrony`

```
sudo service chronyd force-reload
```

- `ntpd`

```
sudo service ntp reload
```

macOS

Pour configurer votre instance ou appareil macOS afin qu'il utilise le Service de synchronisation temporelle d'Amazon public

1. Ouvrez System Preferences (Préférences système).
2. Choisissez Date & Time (Date et heure), puis choisissez l'onglet Date & Time (Date et heure).
3. Pour apporter des modifications, choisissez l'icône en forme de cadenas et saisissez votre mot de passe lorsque vous y êtes invité.
4. Pour Set date and time automatically (Définir automatiquement la date et l'heure), saisissez **time.aws.com**.

Windows

Pour configurer votre instance ou appareil Windows afin qu'il utilise le Service de synchronisation temporelle d'Amazon public

1. Ouvrez le Control Panel (Panneau de configuration).
2. Cliquez sur l'icône Date and Time (Date et heure).
3. Choisissez l'onglet Internet Time (Heure Internet). Cet onglet n'est pas disponible si votre PC fait partie d'un domaine. Dans ce cas, votre PC synchronise l'heure avec le contrôleur de domaine. Vous pouvez configurer le contrôleur pour qu'il utilise le Service de synchronisation temporelle d'Amazon public.
4. Choisissez Change settings (Modifier les paramètres).
5. Cochez la case Synchronize with an Internet time server (Synchroniser avec un serveur de temps Internet).
6. À côté de Server (Serveur), saisissez **time.aws.com**.

Pour configurer votre instance ou appareil Windows Server afin qu'il utilise le Service de synchronisation temporelle d'Amazon public

- Suivez les [instructions de Microsoft](#) (français non disponible) pour mettre à jour votre registre.

Comparez les horodatages de vos instances Linux

Si vous utilisez le service Amazon Time Sync, vous pouvez comparer les horodatages de vos instances Linux Amazon EC2 pour déterminer l'heure réelle ClockBound d'un événement.

ClockBound mesure la précision de l'horloge de votre instance EC2 et vous permet de vérifier si un horodatage donné correspond au passé ou au futur par rapport à l'horloge actuelle de votre instance. Ces informations sont utiles pour déterminer l'ordre et la cohérence des événements et des transactions entre les instances EC2, indépendamment de l'emplacement géographique de chaque instance.

ClockBound est un daemon et une bibliothèque open source. Pour en savoir plus ClockBound, y compris les instructions d'installation, reportez-vous à [ClockBound](#) la section GitHub.

ClockBound n'est pris en charge que pour les instances Linux.

Si vous utilisez la connexion PTP directe à l'horloge matérielle PTP, votre démon temporel, par exemple chrony, sous-estime la limite d'erreur de l'horloge. Cela est dû au fait qu'une horloge matérielle PTP ne transmet pas les informations correctes de limite d'erreur à chrony, comme le fait NTP. Par conséquent, votre démon de synchronisation d'horloge suppose que l'horloge est précise à l'heure UTC et possède donc une limite d'erreur de 0. Pour mesurer la limite d'erreur complète, le système Nitro calcule la borne d'erreur de l'horloge matérielle PTP et la met à la disposition de votre instance EC2 via le système de fichiers du pilote ENA. `sysfs` Vous pouvez le lire directement sous forme de valeur, en nanosecondes.

Pour récupérer la limite d'erreur d'horloge matérielle PTP

1. Trouvez d'abord l'emplacement correct de l'horloge matérielle PTP à l'aide de l'une des commandes suivantes. Le chemin indiqué dans la commande est différent en fonction de l'AMI utilisée pour lancer l'instance.

- Dans Amazon Linux 2:

```
cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
```

- Pour Amazon Linux 2023 :

```
cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
```

La sortie est le nom du slot PCI, qui correspond à l'emplacement de l'horloge matérielle PTP. Dans cet exemple, l'emplacement est `0000:00:03.0`.

```
PCI_SLOT_NAME=0000:00:03.0
```

2. Pour récupérer la limite d'erreur d'horloge matérielle PTP, exécutez la commande suivante. Incluez le nom du slot PCI indiqué à l'étape précédente.

```
cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
```

La sortie correspond à la limite d'erreur d'horloge de l'horloge matérielle PTP, en nanosecondes.

Pour calculer la bonne erreur d'horloge liée à un moment précis lors de l'utilisation de la connexion PTP directe à l'horloge matérielle PTP, vous devez ajouter l'erreur d'horloge liée `ClockBound` à `chrony` ou à l'heure qui `chrony` interroge l'horloge matérielle PTP. Pour plus d'informations sur la mesure et le suivi de la précision de l'horloge, consultez [Gérer la précision de l'horloge des instances Amazon EC2 à l'aide d'Amazon Time Sync Service et d'Amazon CloudWatch — Partie 1](#).

Modifier le fuseau horaire de votre instance

Les instances Amazon EC2 sont définies sur le fuseau horaire UTC (temps universel coordonné) par défaut. Vous pouvez modifier l'heure d'une instance au fuseau horaire local ou à un autre fuseau horaire de votre réseau.

Utilisez les instructions fournies pour le système d'exploitation de votre instance.

Linux

Important

Ces informations s'appliquent à Amazon Linux. Pour obtenir des informations sur d'autres distributions, consultez leur documentation spécifique.

Pour changer le fuseau horaire sur une instance AL2023 ou Amazon Linux 2

1. Affichez le paramètre de fuseau horaire actuel du système.

```
[ec2-user ~]$ timedatectl
```

2. Répertoriez les fuseaux horaires disponibles.

```
[ec2-user ~]$ timedatectl list-timezones
```

3. Définissez le fuseau horaire choisi.

```
[ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
```

4. (Facultatif) Vérifiez que le fuseau horaire actuel est mis à jour vers le nouveau fuseau horaire en ré-exécutant la commande `timedatectl`.

```
[ec2-user ~]$ timedatectl
```

Pour changer le fuseau horaire sur une instance Amazon Linux

1. Identifiez le fuseau horaire à utiliser sur l'instance. Le répertoire `/usr/share/zoneinfo` contient une hiérarchie de fichiers de données sur le fuseau horaire. Parcourez la structure du répertoire à l'endroit où vous recherchez un fichier pour votre fuseau horaire.

```
[ec2-user ~]$ ls /usr/share/zoneinfo
Africa      Chile      GB         Indian     Mideast    posixrules US
America     CST6CDT   GB-Eire    Iran       MST        PRC        UTC
Antarctica  Cuba      GMT        iso3166.tab MST7MDT    PST8PDT    WET
Arctic      EET       GMT0       Israel     Navajo     right      W-SU
...
```

Certaines entrées à cet endroit sont des répertoires (comme `America`), et ces répertoires contiennent des fichiers sur le fuseau horaire pour des villes spécifiques. Recherchez votre ville (ou une ville de votre fuseau horaire) à utiliser pour l'instance.

2. Mettez à jour le fichier `/etc/sysconfig/clock` avec le nouveau fuseau horaire. Dans cet exemple, nous utilisons le fichier de données de fuseau horaire pour Los Angeles, `/usr/share/zoneinfo/America/Los_Angeles`.
 - a. Ouvrez le fichier `/etc/sysconfig/clock` avec un éditeur de texte (tel que `vim` ou `nano`). Vous devez utiliser `sudo` avec la commande de votre éditeur, car `/etc/sysconfig/clock` est détenu par `root`.

```
[ec2-user ~]$ sudo nano /etc/sysconfig/clock
```

- b. Recherchez l'entrée ZONE et remplacez-la par le fichier sur le fuseau horaire (en omettant la section `/usr/share/zoneinfo` du chemin). Par exemple, pour passer au fuseau horaire de Los Angeles, remplacez l'entrée ZONE par ce qui suit:

```
ZONE="America/Los_Angeles"
```

Note

Ne remplacez pas l'entrée `UTC=true` par une autre valeur. Cette entrée concerne l'horloge matérielle et n'a pas besoin d'être corrigée lorsque vous définissez un autre fuseau horaire sur votre instance.

- c. Enregistrez le fichier et quittez l'éditeur de texte.
3. Créez un lien symbolique entre `/etc/localtime` et le fichier de fuseau horaire pour que l'instance trouve le fichier de fuseau horaire lorsqu'il fait référence à des informations sur l'heure locale.

```
[ec2-user ~]$ sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

4. Redémarrez le système pour récupérer les informations sur la nouvelle heure locale dans l'ensemble des services et des applications.

```
[ec2-user ~]$ sudo reboot
```

5. (Facultatif) Vérifiez que le fuseau horaire actuel est mis à jour vers le nouveau fuseau horaire à l'aide de la commande `date`. Le fuseau horaire actuel apparaît dans la sortie. Dans l'exemple suivant, le fuseau horaire actuel est PDT, c'est-à-dire le fuseau horaire de Los Angeles.

```
[ec2-user ~]$ date  
Sun Aug 16 05:45:16 PDT 2020
```

Windows

Pour modifier le fuseau horaire sur une instance Windows

1. Depuis votre instance, ouvrez une fenêtre d'invite de commande.
2. Identifiez le fuseau horaire à utiliser sur l'instance. Pour obtenir une liste des fuseaux horaires, utilisez la commande suivante :

```
tzutil /l
```

Cette commande renvoie une liste de tous les fuseaux horaires disponibles, au format suivant :

```
display name  
time zone ID
```

3. Recherchez l'ID du fuseau horaire à attribuer à l'instance.
4. Attribuez à un autre fuseau horaire à l'aide de la commande suivante :

```
tzutil /s "Pacific Standard Time"
```

Le nouveau fuseau horaire doit prendre effet immédiatement.

Note

Vous pouvez attribuer le fuseau horaire UTC à l'aide de la commande suivante :

```
tzutil /s "UTC"
```

Pour empêcher que votre fuseau horaire ne change une fois que vous l'avez défini pour Windows Server

Lorsque vous modifiez le fuseau horaire d'une instance Windows, vous devez vérifier que le fuseau horaire persiste lors du redémarrage du système. Sinon, lorsque l'instance redémarre, elle recommence à utiliser l'heure universelle coordonnée (UTC). Vous pouvez conserver votre paramètre de fuseau horaire en ajoutant une clé de RealTimeUniversal registre. Cette clé est définie par défaut sur toutes les instances de génération en cours. Pour vérifier si la clé de Registre

RealTimelsUniversal est définie, consultez l'étape 4 de la procédure suivante. Si la clé n'est pas définie, procédez comme suit depuis le début.

Pour définir la clé RealTimelsUniversal de registre

1. Depuis l'instance, ouvrez une fenêtre d'invite de commande.
2. Cette commande vous permet d'ajouter la clé de registre :

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. Si vous utilisez une AMI Windows Server 2008 (et non Windows Server 2008 R2) créée avant le 22 février 2013, nous vous recommandons de passer à la dernière AMI AWS Windows. Si vous utilisez une AMI exécutant Windows Server 2008 R2 (pas Windows Server 2008), vous devez vérifier que le correctif Microsoft [KB2922223](#) est installé. Si ce correctif n'est pas installé, nous vous recommandons de passer à la dernière version de l'AMI AWS Windows.
4. (Facultatif) Vérifiez que l'instance a enregistré la clé à l'aide de la commande suivante :

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /s
```

Cette commande renvoie les sous-clés de la clé de registre TimeZoneInformation. La clé RealTimelsUniversal doit s'afficher en bas de la liste, comme suit :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                REG_DWORD    0x1e0
    DaylightBias        REG_DWORD    0xffffffffc4
    DaylightName        REG_SZ       @tzres.dll,-211
    DaylightStart       REG_BINARY   00000300020002000000000000000000
    StandardBias        REG_DWORD    0x0
    StandardName        REG_SZ       @tzres.dll,-212
    StandardStart       REG_BINARY   00000B00010002000000000000000000
    TimeZoneKeyName    REG_SZ       Pacific Standard Time
    DynamicDaylightTimeDisabled REG_DWORD    0x0
    ActiveTimeBias      REG_DWORD    0x1a4
    RealTimeIsUniversal REG_DWORD    0x1
```

Secondes intercalaires

Les secondes intercalaires, introduites en 1972, sont des ajustements occasionnels d'une seconde de l'heure UTC pour tenir compte des irrégularités de la rotation de la Terre et, par conséquent, des différences entre le temps atomique international (TAI) et le temps solaire (Ut1). Pour gérer les secondes intercalaires pour le compte des clients, nous avons conçu la correction des secondes intercalaires au sein du Service de synchronisation temporelle d'Amazon. Pour plus d'informations, consultez le billet de blog [Look Before You Leap – The Coming Leap Second and AWS](#).

Les secondes intercalaires sont en train de disparaître, et nous soutenons pleinement la décision prise lors de la [27e Conférence générale des poids et mesures d'abandonner les secondes intercalaires d'ici 2035](#).

Pour faciliter cette transition, nous prévoyons toujours de corriger le temps en cas d'ajout d'une seconde intercalaire lors de l'accès au Service de synchronisation temporelle d'Amazon via la connexion NTP locale ou via nos groupes NTP publics (`time.aws.com`). Toutefois, l'horloge matérielle PTP ne propose pas d'option d'horaire corrigé. En cas de seconde intercalaire, l'horloge matérielle PTP ajoute la seconde intercalaire conformément aux normes UTC. Les sources temporelles à seconde intercalaire corrigées et non corrigées sont généralement identiques. Toutefois, étant donné qu'elles diffèrent en cas d'ajout de seconde intercalaire, nous vous déconseillons d'utiliser à la fois des sources temporelles corrigées et non corrigées dans la configuration de votre client temporel lors de l'ajout d'une seconde intercalaire.

Ressources connexes

- AWS Blog informatique : [Il était temps : des horloges précises à la microseconde sur les instances Amazon EC2](#)
- (Linux) <https://chrony-project.org/>
- (Windows) [Fonctionnement du service Windows Time](#) (Microsoft)
- (Windows) [W32™](#) (Microsoft)
- (Windows) [Comment le service Windows Time traite une seconde intercalaire](#) (Microsoft)
- (Windows) [L'histoire de Leap Seconds et de Windows : ce n'est probablement pas le passage à l'an 2000](#) (Microsoft)

Contrôle de l'état du processeur pour votre instance Linux Amazon EC2

Les états « C-state » contrôlent les niveaux de veille dans lesquels un cœur peut entrer lorsqu'il est inutilisé. Les états « C-state » sont numérotés de C0 (l'état le plus superficiel lorsque le cœur est totalement éveillé et exécute les instructions) à C6 (l'état de veille le plus profond lorsqu'un cœur est arrêté).

Les états « P-states » contrôlent les performances souhaitées (dans la fréquence de l'UC) à partir d'un cœur. La numérotation des états « P-states » commence à P0 (paramètre de performance le plus élevé dans lequel le cœur peut utiliser la technologie Intel Turbo Boost pour améliorer la fréquence si possible) et va de P1 (état « P-state » qui demande la fréquence de base maximale) à P15 (fréquence la plus basse possible).

États C-state et P-state

Les types d'instance EC2 suivants permettent à un système d'exploitation de contrôler les états « C-state » et « P-state » des processeurs.

- Usage général : m4.10xlarge m4.16xlarge | m5.metal m5d.metal | m5n.metal | m5zn.metal | m6i.metal | m6id.metal | m7a.metal-48x1 | m7i.metal-24x1 | m7i.metal-48x1
- Calcul optimisé : c4.8xlarge | c5.metal | c5an.metal | c5adn.metal | c5n.metal | c6i.metal | c6id.metal | c7a.metal-48x1 | c7i.metal-24x1 | c7i.metal-48x1
- Mémoire optimisée : r4.8xlarge | r4.16xlarge | r5.metal | r5b.metal | r5d.metal | r6i.metal | r7a.metal-48x1 | r7i.metal-24x1 | r7i.metal-48x1 | r7iz.metal-16x1 | r7iz.metal-32x1 | u-6tb1.metal | u-9tb1.metal | u-12tb1.metal | u-18tb1.metal | u-24tb1.metal | x1.16xlarge | x1.32xlarge | x1e.8xlarge | x1e.16xlarge | x1e.32xlarge | z1d.metal
- Stockage optimisé: d2.8xlarge | d3.metal | d3en.metal | i3.8xlarge | i3.16xlarge | i3.metal | i3en.metal | h1.8xlarge | h1.16xlarge
- Calcul accéléré: f1.16xlarge | g3.16xlarge | g4dn.metal | p2.16xlarge | p3.16xlarge

États C-state uniquement

Les types d'instance suivants permettent à un système d'exploitation de contrôler les états « C-state » des processeurs :

- Usage général : m5.12xlarge m5.24xlarge m5d.12xlarge | m5d.24xlarge | m5n.12xlarge | m5n.24xlarge | m5dn.12xlarge | m5dn.24xlarge | m6a.24xlarge | m6a.48xlarge m6ad.metal | m6i.16xlarge | m6i.32xlarge | m7a.medium | m7a.large | m7a.xlarge | m7a.2xlarge | m7a.4xlarge m7a.8xlarge | m7a.12xlarge | m7a.16xlarge | m7a.24xlarge | m7a.32xlarge | m7a.48xlarge | m7i.large | m7i.xlarge | m7i.2xlarge | m7i.4xlarge | m7i.8xlarge | m7i.12xlarge | m7i.16xlarge | m7i.24xlarge | m7i.48xlarge
- Optimisé pour le calcul : c5.9xlarge c5.12xlarge c5.18xlarge c5.24xlarge c5a.24xlarge | c5ad.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5n.9xlarge c5n.18xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge | c6i.16xlarge | c6i.32xlarge | c7a.medium | c7a.large | c7a.xlarge | c7a.2xlarge c7a.4xlarge | c7a.8xlarge | c7a.12xlarge | c7a.16xlarge | c7a.24xlarge | c7a.32xlarge | c7a.48xlarge | c7i.large | c7i.xlarge | c7i.2xlarge c7i.4xlarge | c7i.8xlarge | c7i.12xlarge | c7i.16xlarge | c7i.24xlarge | c7i.48xlarge
- Mémoire optimisée : r5.12xlarge | r5.24xlarge | r5d.12xlarge | r5d.24xlarge | r5n.12xlarge | r5n.24xlarge | r5dn.12xlarge | r5dn.24xlarge | r6a.24xlarge | r6a.48xlarge | r6i.16xlarge | r6i.32xlarge | r6id.32xlarge | r6in.32xlarge | r7a.medium | r7a.large | r7a.xlarge | r7a.2xlarge | r7a.4xlarge | r7a.8xlarge | r7a.12xlarge | r7a.16xlarge | r7a.24xlarge | r7a.32xlarge | r7a.48xlarge | r7i.large | r7i.xlarge | r7i.2xlarge | r7i.4xlarge | r7i.8xlarge | r7i.12xlarge | r7i.16xlarge | r7i.24xlarge | r7i.48xlarge | r7iz.large | r7iz.xlarge | r7iz.2xlarge | r7iz.4xlarge | r7iz.8xlarge r7iz.12xlarge | r7iz.16xlarge | r7iz.32xlarge | u-6tb1.56xlarge | u-6tb1.112xlarge u-9tb1.112xlarge | u-12tb1.112xlarge | u-18tb1.112xlarge | u-24tb1.112xlarge | u7i-12tb.224xlarge | u7in-16tb.224xlarge u7in-24tb.224xlarge | u7in-32tb.224xlarge | z1d.6xlarge | z1d.12xlarge
- Stockage optimisé : d3en.12xlarge | dl1.24xlarge | i3en.12xlarge | i3en.24xlarge | i4i.metal | r5b.12xlarge | r5b.24xlarge | i4i.16xlarge
- Calcul accéléré : dl1.24xlarge g5.24xlarge | g5.48xlarge g6.24xlarge | g6.48xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge | vt1.24xlarge

AWS Les processeurs Graviton sont dotés de modes d'économie d'énergie intégrés et fonctionnent à une fréquence fixe. Par conséquent, ils ne permettent pas au système d'exploitation de contrôler les états « C-state » et les états « P-state ».

Il se peut que vous vouliez changer les paramètres « C-state » ou « P-state » pour améliorer la cohérence des performances du processeur, réduire la latence ou ajuster votre instance pour une charge de travail spécifique. Les paramètres « C-state » ou « P-state » par défaut offre des performances maximales qui sont optimales pour la plupart des charges de travail. Cependant, si votre application tirerait avantage de la latence réduite pour un coût de fréquences simple ou double cœur plus hautes ou des performances cohérentes à des fréquences plus basses au lieu des fréquences Turbo Boost transmises en paquets, pensez à essayer les paramètres « C-state » ou « P-state » qui sont disponibles pour ces instances.

Pour plus d'informations sur les différentes configurations de processeur et sur la manière de surveiller les effets de votre configuration pour Amazon Linux, consultez la section [Contrôle de l'état du processeur pour l'instance Amazon EC2 Amazon Linux](#) dans le guide de l'utilisateur Amazon Linux 2. Ces procédures ont été écrites pour Amazon Linux et s'appliquent à celui-ci ; toutefois, elles peuvent également fonctionner pour d'autres distributions Linux avec un noyau Linux de version 3.9 ou ultérieure. Pour obtenir plus d'informations sur les autres distributions Linux et le contrôle des états du processeur, consultez la documentation spécifique à votre système.

Optimiser les options d'UC

Les instances Amazon EC2 prennent en charge le multithreading, qui permet l'exécution simultanée de plusieurs threads sur un seul cœur d'UC. Chaque thread est représenté comme UC virtuelle (vCPU) sur l'instance. Une instance possède un certain nombre par défaut de cœurs d'UC, qui varie en fonction du type d'instance. Par exemple, un type d'instance `m5.xlarge` a deux cœurs d'UC et deux threads par cœur par défaut, quatre vCPU— au total.

Note

Chaque processeur virtuel est un thread d'un cœur d'UC, sauf pour les instances T2, les instances M7a, les instances Apple Silicon Mac et les plateformes ARM 64 bits telles que les instances équipées de processeurs AWS Graviton.

Dans la plupart des cas, il y a un type d'instance Amazon EC2 qui possède une combinaison de mémoire et d'un certain nombre de vCPU pour convenir à vos charges de travail. Cependant, vous pouvez spécifier les options d'UC suivantes pour optimiser votre instance pour des besoins métier ou des charges de travail spécifiques :

- **Nombre de cœurs d'UC** : vous pouvez personnaliser le nombre de cœurs d'UC pour l'instance. Vous pourriez agir ainsi pour optimiser potentiellement les coûts de licence de vos logiciels avec une instance ayant une quantité suffisante de RAM pour les charges de travail exigeantes en mémoire, mais moins de cœurs d'UC.
- **Threads per core (Threads par cœur)** : vous pouvez désactiver le multithreading en spécifiant un seul thread par cœur d'UC. Vous pourriez agir ainsi pour certaines charges de travail, telles que les charges de travail de calcul haute performance (HPC).

Vous pouvez spécifier ces options d'UC lors du lancement de l'instance. Il n'y a pas de frais supplémentaires ou réduits pour spécifier des options d'UC. Vous êtes facturé de la même façon que pour les instances lancées avec les options d'UC par défaut.

Sommaire

- [Règles pour spécifier les options d'UC](#)
- [Cœurs d'UC et threads par cœur d'UC par type d'instance](#)
- [Spécifier les options d'UC pour votre instance](#)
- [Afficher les options d'UC pour votre instance](#)

Règles pour spécifier les options d'UC

Pour spécifier les options d'UC pour votre instance, soyez conscient des règles suivantes :

- Vous ne pouvez pas spécifier d'options de processeur pour les instances de matériel nu.
- Les options d'UC ne peuvent être spécifiées que pendant un lancement d'instance et ne peuvent pas être modifiées après le lancement.
- Lorsque vous lancez une instance, vous devez spécifier le nombre de cœurs d'UC et de threads par cœur dans la demande. Pour obtenir des exemples de requête, consultez [Spécifier les options d'UC pour votre instance](#).
- Le nombre de vCPU pour l'instance est égal au nombre de cœurs d'UC multiplié par le nombre de threads par cœur. Pour spécifier un nombre personnalisé de vCPU, vous devez spécifier un nombre valide de cœurs d'UC et de threads par cœur pour le type d'instance. Vous ne pouvez pas dépasser le nombre de vCPU par défaut pour l'instance. Pour plus d'informations, consultez [Cœurs d'UC et threads par cœur d'UC par type d'instance](#).
- Pour désactiver le multithreading, spécifiez un seul thread par cœur.

- Si vous [modifiez le type d'une instance](#) existante, les options d'UC se changent automatiquement en options d'UC par défaut pour le nouveau type d'instance.
- Les options d'UC spécifiées sont conservées après que vous arrêtez, démarrez ou redémarrez une instance.

Cœurs d'UC et threads par cœur d'UC par type d'instance

Les tableaux suivants répertorient les types d'instance qui prennent en charge la spécification des options d'UC.

Table des matières

- [instances à usage général](#)
- [instances de calcul optimisé](#)
- [instances de mémoire optimisée](#)
- [instances de stockage optimisé](#)
- [instances à calcul accéléré](#)
- [Instances de calcul hautes performances](#)

instances à usage général

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m2.xlarge	2	2	1	1, 2	1
m2.2xlarge	4	4	1	1, 2, 3, 4	1
m2.4xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m3.large	2	1	2	1	1, 2
m3.xlarge	4	2	2	1, 2	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2	1	2	1	1, 2
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6a.large	2	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6id.large	2	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
m7i-flex.large	2	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
t3.nano	2	1	2	1	1, 2
t3.micro	2	1	2	1	1, 2
t3.small	2	1	2	1	1, 2
t3.medium	2	1	2	1	1, 2
t3.large	2	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2	1	2	1	1, 2
t3a.micro	2	1	2	1	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

instances de calcul optimisé

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c3.large	2	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c4.large	2	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c6a.large	2	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1, 2, 3, 4	1
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6id.large	2	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
c7i-flex.large	2	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

instances de mémoire optimisée

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r3.large	2	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r5dn.xlarge	4	2	2	1, 2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6idn.large	2	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2	1	2	1	1, 2
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7iz.large	2	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
u-3tb1.56xlarge	224	112	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2
u-6tb1.56xlarge	224	224	1	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
u-6tb1.11 2xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-9tb1.11 2xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
u-12tb1.1 12xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-18tb1.1 12xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
u-24tb1.1 12xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
u7i-12tb. 224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
u7in-16tb .224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
u7in-24tb .224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
u7in-32tb .224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
z1d.large	2	1	2	1	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
z1d.xlarge	4	2	2	1, 2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

instances de stockage optimisé

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
i3.large	2	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
i3en.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
i4g.large	2	2	1	1, 2	1
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

instances à calcul accéléré

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28,	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
				30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
f1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
f1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
p2.xlarge	4	2	2	1, 2	1, 2
p2.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p2.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
p3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
trn1.2xlarge	8	4	2	2, 4	1, 2
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

Instances de calcul hautes performances

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
hpc6id.32xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46,	1

Type d'instance	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Cœurs d'UC valides	Threads valides par cœur
				48, 50, 52, 54, 56, 58, 60, 62, 64	

Spécifier les options d'UC pour votre instance

Vous pouvez spécifier les options d'UC lors du lancement de l'instance.

[Les exemples suivants décrivent comment spécifier les options du processeur lors de l'utilisation de l'assistant de lancement d'instance dans la console EC2 et de la AWS CLI commande `run-instances`, ainsi que de la page de création d'un modèle de lancement dans la console EC2 et de la commande `create-launch-template`.](#) AWS CLI Pour les flottes EC2 ou les parcs d'instances Spot, vous devez spécifier les options du processeur dans un modèle de lancement.

Les exemples suivants concernent un type d'instance `r5.4xlarge`, qui possède les [valeurs par défaut suivantes](#) :

- Cœurs d'UC par défaut : 8
- Threads par défaut par cœur : 2
- vCPU par défaut : 16 (8*2)
- Nombre valide de cœurs de processeur : 2, 4, 6, 8
- Nombre valide de threads par cœur : 1, 2

Désactiver le multithreading

Pour désactiver le multithreading, spécifiez 1 thread par cœur.

New console

Désactiver le multithreading pendant le lancement d'une instance

1. Suivez la procédure [Lancer rapidement une instance](#) et configurez votre instance selon vos besoins.
2. Développez Informations avancées et cochez la case Spécifier les options du processeur.

3. Sous Core count (Nombre de cœurs), choisissez le nombre de cœurs d'UC requis. Dans cet exemple, pour spécifier le nombre de cœurs d'UC par défaut pour une instance `r5.4xlarge`, choisissez 8.
4. Pour désactiver le multithreading, sous Threads per core (Threads par cœur), sélectionnez 1.
5. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Old console

Désactiver le multithreading pendant le lancement d'une instance

1. Suivez la procédure [Lancer une instance à l'aide de l'ancien assistant de lancement d'instance](#).
2. Sur la page Configurer les détails de l'instance, sous CPU options (Options d'UC), choisissez Specify CPU options (Spécifier les options d'UC).
3. Sous Core count (Nombre de cœurs), choisissez le nombre de cœurs d'UC requis. Dans cet exemple, pour spécifier le nombre de cœurs d'UC par défaut pour une instance `r5.4xlarge`, choisissez 8.
4. Pour désactiver le multithreading, sous Threads per core (Threads par cœur), sélectionnez 1.
5. Continuez comme indiqué par l'assistant. Lorsque vous avez terminé de vérifier vos options sur la page Examiner le lancement de l'instance, choisissez Lancer. Pour plus d'informations, consultez [Lancer une instance à l'aide de l'ancien assistant de lancement d'instance](#).

AWS CLI

Désactiver le multithreading pendant le lancement d'une instance

Utilisez la commande [run-instances](#) de l'AWS CLI et spécifiez la valeur 1 pour `ThreadsPerCore` pour le paramètre `--cpu-options`. Pour `CoreCount`, spécifiez le nombre de cœurs d'UC. Dans cet exemple, pour spécifier le nombre de cœurs d'UC par défaut pour une instance `r5.4xlarge`, spécifiez la valeur 8.

```
aws ec2 run-instances \  
  --image-id ami-1a2b3c4d \  
  --instance-type r5.4xlarge \  
  --cpu-options "CoreCount=8,ThreadsPerCore=1" \  
  --
```

```
--key-name MyKeyPair
```

Spécifiez un nombre personnalisé de vCPU au lancement

Vous pouvez personnaliser le nombre de cœurs d'UC et de threads par cœur pour l'instance.

L'exemple suivant lance une `r5.4xlarge` instance avec 4 vCPU.

New console

Pour spécifier un nombre personnalisé de vCPU lors du lancement de l'instance

1. Suivez la procédure [Lancer rapidement une instance](#) et configurez votre instance selon vos besoins.
2. Développez Informations avancées et cochez la case Spécifier les options du processeur.
3. Pour obtenir 4 vCPU, spécifiez 2 cœurs de processeur et 2 threads par cœur, comme suit :
 - Pour Nombre de cœurs, choisissez 2.
 - Sous Threads per core (Threads par cœur), choisissez 2.
4. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Old console

Pour spécifier un nombre personnalisé de vCPU lors du lancement de l'instance

1. Suivez la procédure [Lancer une instance à l'aide de l'ancien assistant de lancement d'instance](#).
2. Sur la page Configurer les détails de l'instance, sous CPU options (Options d'UC), choisissez Specify CPU options (Spécifier les options d'UC).
3. Pour obtenir 4 vCPU, spécifiez 2 cœurs de processeur et 2 threads par cœur, comme suit :
 - Pour Nombre de cœurs, choisissez 2.
 - Sous Threads per core (Threads par cœur), choisissez 2.

4. Continuez comme indiqué par l'assistant. Lorsque vous avez terminé de vérifier vos options sur la page Examiner le lancement de l'instance, choisissez Lancer. Pour plus d'informations, consultez [Lancer une instance à l'aide de l'ancien assistant de lancement d'instance](#).

AWS CLI

Pour spécifier un nombre personnalisé de vCPU lors du lancement de l'instance

Utilisez la AWS CLI commande [run-instances](#) et spécifiez le nombre de cœurs de processeur et le nombre de threads dans le `--cpu-options` paramètre. Vous pouvez spécifier 2 cœurs de processeur et 2 threads par cœur pour obtenir 4 vCPU.

```
aws ec2 run-instances \  
  --image-id ami-1a2b3c4d \  
  --instance-type r5.4xlarge \  
  --cpu-options "CoreCount=2,ThreadsPerCore=2" \  
  --key-name MyKeyPair
```

Vous pouvez également spécifier 4 cœurs de processeur et 1 thread par cœur (désactiver le multithreading) pour obtenir 4 vCPU :

```
aws ec2 run-instances \  
  --image-id ami-1a2b3c4d \  
  --instance-type r5.4xlarge \  
  --cpu-options "CoreCount=4,ThreadsPerCore=1" \  
  --key-name MyKeyPair
```

Spécifier un nombre personnalisé de vCPU dans un modèle de lancement

Vous pouvez personnaliser le nombre de cœurs de CPU et de threads par cœur pour l'instance dans un modèle de lancement.

L'exemple suivant crée un modèle de lancement qui spécifie la configuration d'une `r5.4xlarge` instance avec 4 vCPU.

Console

Pour spécifier un nombre personnalisé de vCPU dans un modèle de lancement

1. Suivez la procédure [Création d'un modèle de lancement à partir de paramètres](#) et configurez votre modèle de lancement selon vos besoins.
2. Développez Informations avancées et cochez la case Spécifier les options du processeur.
3. Pour obtenir 4 vCPU, spécifiez 2 cœurs de processeur et 2 threads par cœur, comme suit :
 - Pour Nombre de cœurs, choisissez 2.
 - Sous Threads per core (Threads par cœur), choisissez 2.
4. Dans le panneau Résumé, vérifiez la configuration de votre instance, puis choisissez Créer un modèle de lancement. Pour plus d'informations, consultez [Lancer une instance à partir d'un modèle de lancement](#).

AWS CLI

Pour spécifier un nombre personnalisé de vCPU dans un modèle de lancement

Utilisez la AWS CLI commande [create-launch-template](#) et spécifiez le nombre de cœurs de processeur et le nombre de threads dans le paramètre. `CpuOptions` Vous pouvez spécifier 2 cœurs de processeur et 2 threads par cœur pour obtenir 4 vCPU.

```
aws ec2 create-launch-template \  
  --launch-template-name TemplateForCPUOptions \  
  --version-description CPUOptionsVersion1 \  
  --launch-template-data file://template-data.json
```

Vous trouverez ci-dessous un exemple de fichier JSON contenant les données du modèle de lancement, qui inclut les options CPU, pour la configuration de l'instance de cet exemple.

```
{  
  "NetworkInterfaces": [{  
    "AssociatePublicIpAddress": true,  
    "DeviceIndex": 0,  
    "Ipv6AddressCount": 1,  
    "SubnetId": "subnet-7b16de0c"  
  }],  
  "ImageId": "ami-8c1be5f6",  
  "InstanceType": "r5.4xlarge",
```

```

    "TagSpecifications": [{
      "ResourceType": "instance",
      "Tags": [{
        "Key": "Name",
        "Value": "webserver"
      }]
    }],
    "CpuOptions": {
      "CoreCount": 2,
      "ThreadsPerCore": 2
    }
  }
}

```

Vous pouvez également spécifier 4 cœurs de processeur et 1 thread par cœur (désactiver le multithreading) pour obtenir 4 vCPU :

```

{
  "NetworkInterfaces": [{
    "AssociatePublicIpAddress": true,
    "DeviceIndex": 0,
    "Ipv6AddressCount": 1,
    "SubnetId": "subnet-7b16de0c"
  }],
  "ImageId": "ami-8c1be5f6",
  "InstanceType": "r5.4xlarge",
  "TagSpecifications": [{
    "ResourceType": "instance",
    "Tags": [{
      "Key": "Name",
      "Value": "webserver"
    }]
  }],
  "CpuOptions": {
    "CoreCount": 4,
    "ThreadsPerCore": 1
  }
}

```

Afficher les options d'UC pour votre instance

Vous pouvez afficher les options d'UC pour une instance existante dans la console Amazon EC2 ou en décrivant l'instance à l'aide de la AWS CLI.

Console

Pour afficher les options d'UC d'une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation sur la gauche, choisissez Instances, puis sélectionnez l'instance.
3. Sous l'onglet Détails, sous Hôte et groupe de placement, recherchez Nombre de vCPU.

AWS CLI

Pour afficher les options d'UC pour une instance (AWS CLI)

Utilisez la commande [describe-instances](#).

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

```
...
  "Instances": [
    {
      "Monitoring": {
        "State": "disabled"
      },
      "PublicDnsName": "ec2-198-51-100-5.eu-central-1.compute.amazonaws.com",
      "State": {
        "Code": 16,
        "Name": "running"
      },
      "EbsOptimized": false,
      "LaunchTime": "2018-05-08T13:40:33.000Z",
      "PublicIpAddress": "198.51.100.5",
      "PrivateIpAddress": "172.31.2.206",
      "ProductCodes": [],
      "VpcId": "vpc-1a2b3c4d",
      "CpuOptions": {
        "CoreCount": 34,
        "ThreadsPerCore": 1
      },
      "StateTransitionReason": "",
      ...
    }
  ]
}
```

]

...

Dans le résultat retourné, le champ `CoreCount` indique le nombre de cœurs pour l'instance. Le champ `ThreadsPerCore` indique le nombre de threads par cœur.

Pour consulter les informations relatives au processeur, vous pouvez également vous connecter à votre instance et utiliser l'un des outils système suivants :

- Windows Task Manager sur votre instance Windows
- La `lscpu` commande sur votre instance Linux

Vous pouvez l'utiliser AWS Config pour enregistrer, évaluer, auditer et évaluer les modifications de configuration des instances, y compris les instances résiliées. Pour plus d'informations, consultez [Mise en route avec AWS Config](#) dans le AWS Config Guide du développeur.

AMD SEV-SNP sur Amazon EC2

AMD Secure Encrypted Virtualization-Secure Nested Paging (AMD SEV-SNP) est une fonction du processeur qui fournit les propriétés suivantes :

- **Attestation** : AMD SEV-SNP vous permet de récupérer un rapport d'attestation signé contenant une mesure cryptographique pouvant être utilisée pour valider l'état et l'identité de l'instance, et indiquant qu'elle s'exécute sur du matériel AMD authentique. Pour plus d'informations, consultez [Attestation avec AMD SEV-SNP](#).
- **Chiffrement de la mémoire** : à partir des processeurs AMD EPYC (Milan), AWS Graviton2 et Intel Xeon Scalable (Ice Lake), la mémoire de l'instance est toujours chiffrée. Les instances activées pour AMD SEV-SNP utilisent une clé spécifique à l'instance pour le chiffrement de leur mémoire.

Concepts et terminologie

Avant de commencer à utiliser AMD SEV-SNP, assurez-vous de vous familiariser avec les concepts et la terminologie suivants.

Rapport d'attestation AMD SEV-SNP

Le rapport d'attestation AMD SEV-SNP est un document qu'une instance peut demander au processeur. Le rapport d'attestation AMD SEV-SNP peut être utilisé pour valider l'état et l'identité

d'une instance et pour vérifier qu'elle s'exécute dans un environnement AMD agréé. Le rapport inclut une mesure de lancement, qui est un hachage cryptographique de l'état de démarrage initial d'une instance, y compris le contenu de la mémoire de l'instance initiale et l'état initial des vCPU. Le rapport d'attestation AMD SEV-SNP est signé par une signature VLEK qui renvoie à une racine de confiance AMD.

VLEK

La VLEK (Versioned Loaded Endorsement Key) est une clé de signature versionnée, certifiée par AMD et utilisée par le processeur AMD pour signer les rapports d'attestation AMD SEV-SNP. Les signatures VLEK peuvent être validées à l'aide de certificats fournis par AMD.

OVMF binaire

L'OVMF (Open Virtual Machine Firmware) est le code de démarrage anticipé utilisé pour fournir un environnement UEFI à l'instance. Le code de démarrage anticipé est exécuté avant le démarrage du code de l'AMI. L'OVMF trouve et exécute également le chargeur de démarrage fourni dans l'AMI. Pour plus d'informations, consultez le [référentiel OVMF](#) (français non garanti).

Prérequis

Pour utiliser AMD SEV-SNP, vous devez procéder comme suit :

- Utilisez l'un des types d'instance pris en charge suivants :
 - Usage général : `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
 - Optimisées pour le calcul : `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
 - Mémoire optimisée : `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Lancez votre instance dans un environnement compatible Région AWS. À l'heure actuelle, seules les régions USA Est (Ohio) et Europe (Irlande) sont prises en charge.
- Utilisez une AMI avec le mode de démarrage `uefi` ou `uefi-preferred` et un système d'exploitation qui prend en charge AMD SEV-SNP. Pour plus d'informations sur la prise en charge d'AMD SEV-SNP sur votre système d'exploitation, consultez la documentation du système d'exploitation correspondant. En effet AWS, AMD SEV-SNP est pris en charge sur AL2023, RHEL 9.3, SLES 15 SP4 et Ubuntu 23.04 et versions ultérieures.

Considérations

Vous ne pouvez activer AMD SEV-SNP que lorsque vous lancez une instance. Lorsque AMD SEV-SNP est activé pour le lancement de votre instance, les règles suivantes s'appliquent.

- L'AMD SEV-SNP ne peut pas être désactivé. Elle reste active tout au long du cycle de vie de l'instance.
- Vous ne pouvez [modifier le type d'instance](#) que pour un autre type d'instance compatible avec AMD SEV-SNP.
- Hibernation et Nitro Enclaves ne sont pas pris en charge.
- Les hôtes dédiés ne sont pas pris en charge.
- Si la maintenance de l'hôte sous-jacent de votre instance est planifiée, vous recevrez une notification d'événement planifié 14 jours avant l'événement. Vous devez arrêter ou redémarrer manuellement votre instance pour la déplacer vers un nouvel hôte.

Tarifification

Lorsque vous lancez une instance Amazon EC2 avec AMD SEV-SNP activé, des frais d'utilisation horaires supplémentaires équivalents à 10 % du [taux horaire à la demande](#) du type d'instance sélectionné vous sont facturés.

Ces frais d'utilisation d'AMD SEV-SNP sont des frais distincts liés à l'utilisation de votre instance Amazon EC2. Les instances réservées, les Savings Plans et l'utilisation du système d'exploitation n'ont aucune incidence sur ces frais.

Si vous configurez une instance Spot pour qu'elle soit lancée avec [AMD SEV-SNP](#) activé, des frais d'utilisation horaires supplémentaires vous seront facturés, équivalant à 10 % du [taux horaire à la demande](#) du type d'instance sélectionné. Si la stratégie d'allocation utilise le prix comme entrée, le parc d'instances Spot n'inclut pas ces frais supplémentaires ; seul le prix au comptant est utilisé.

Travaillez avec AMD SEV-SNP sur Amazon EC2

Effectuez les tâches suivantes pour travailler avec AMD SEV-SNP sur Amazon EC2.

Tâches

- [Rechercher les types d'instances pris en charge](#)
- [Activer AMD SEV-SNP lors du lancement](#)

- [Vérifier l'état d'AMD SEV-SNP](#)

Rechercher les types d'instances pris en charge

Vous pouvez utiliser le AWS CLI pour rechercher les types d'instances compatibles avec AMD SEV-SNP.

Pour rechercher les types d'instances compatibles avec AMD SEV-SNP à l'aide de AWS CLI, utilisez la commande suivante. [describe-instance-types](#)

```
$ C:\> aws ec2 describe-instance-types \
--filters Name=processor-info.supported-features,Values=amd-sev-snp \
--query 'InstanceTypes[*].InstanceType'
```

Exemple de sortie.

```
[
  "r6a.2xlarge",
  "m6a.large",
  "m6a.2xlarge",
  "r6a.xlarge",
  "c6a.16xlarge",
  "c6a.8xlarge",
  "m6a.4xlarge",
  "c6a.12xlarge",
  "r6a.4xlarge",
  "c6a.xlarge",
  "c6a.4xlarge",
  "c6a.2xlarge",
  "m6a.xlarge",
  "c6a.large",
  "r6a.large",
  "m6a.8xlarge"
]
```

Activer AMD SEV-SNP lors du lancement

Vous pouvez utiliser le AWS CLI pour lancer une instance avec AMD SEV-SNP activé.

Pour lancer une instance avec AMD SEV-SNP activé à l'aide de AWS CLI, utilisez la [run-instances](#) commande et incluez l'option. `--cpu-options AmdSevSnp=enabled` Pour `--image-`

id, spécifiez une AMI avec le mode de démarrage uefi ou uefi-preferred boot et un système d'exploitation qui prend en charge AMD SEV-SNP. Pour `--instance-type`, spécifiez un type d'instance pris en charge.

```
$ C:\> aws ec2 run-instances \  
--image-id supported_ami_id \  
--instance-type supported_instance_type \  
--key-name key_pair_name \  
--subnet-id subnet_id \  
--cpu-options AmdSevSnp=enabled
```

Vérifier l'état d'AMD SEV-SNP

Vous pouvez utiliser l'une des méthodes suivantes pour vérifier l'état d'AMD SEV-SNP.

AWS CLI

Pour vérifier si AMD SEV-SNP est activé pour une instance à l'aide de AWS CLI, utilisez la commande. [describe-instances](#) Pour `--instance-ids`, spécifiez l'ID de l'instance à vérifier.

```
$ C:\> aws ec2 describe-instances --instance-ids instance_id
```

Dans la sortie de commande, la valeur de `AmdSevSnp` dans `CpuOptions` indique si AMD SEV-SNP est activé ou désactivé.

AWS CloudTrail

En AWS CloudTrail cas de demande de lancement d'instance, une valeur de `"cpuOptions"` : `{"AmdSevSnp": enabled}` indique qu'AMD SEV-SNP est activé pour l'instance.

Attestation avec AMD SEV-SNP

L'attestation est un processus qui permet à votre instance de prouver son état et son identité. Lorsque vous activez AMD SEV-SNP pour votre instance, vous pouvez demander un rapport d'attestation AMD SEV-SNP au processeur sous-jacent. Le rapport d'attestation AMD SEV-SNP contient un hachage cryptographique (appelé mesure de lancement) du contenu initial de la mémoire client et de l'état initial du vCPU. Le rapport d'attestation est signé avec une signature VLEK qui renvoie à une source de confiance AMD. Vous pouvez utiliser la mesure de lancement incluse dans le rapport d'attestation pour vérifier que l'instance s'exécute dans un environnement AMD authentique et pour valider le code de démarrage initial qui a été utilisé pour lancer l'instance.

Pour effectuer une attestation avec AMD SEV-SNP, procédez comme suit.

Étape 1 : obtention du rapport d'attestation

Au cours de cette étape, vous installez et compilez l'`snpquest` utilitaire, puis vous l'utilisez pour demander le rapport d'attestation et les certificats AMD SEV-SNP.

1. Exécutez les commandes suivantes pour créer l'`snpquest` utilitaire à partir du [snpquest repository](#).

```
$ C:\> git clone https://github.com/virtee/snpquest.git
$ C:\> cd snpquest
$ C:\> cargo build -r
$ C:\> cd target/release
```

2. Générez une demande pour le rapport d'attestation. L'utilitaire demande le rapport d'attestation à l'hôte et l'écrit dans un fichier binaire avec les données de demande fournies.

L'exemple suivant crée une chaîne de requête aléatoire et l'utilise comme fichier de demande (`request-file.txt`). Lorsque la commande renvoie le rapport d'attestation, celui-ci est stocké dans le chemin de fichier que vous spécifiez (`report.bin`). Dans ce cas, l'utilitaire enregistre le rapport dans le répertoire courant.

```
$ C:\> ./snpquest report report.bin request-file.txt --random
```

3. Demandez les certificats à la mémoire de l'hôte et stockez-les sous forme de fichiers PEM. L'exemple suivant enregistre les fichiers dans le même répertoire que l'`snpquest` utilitaire. Si des certificats existent déjà dans le répertoire spécifié, ils sont remplacés.

```
$ C:\> ./snpquest certificates PEM ./
```

Étape 2 : Valider la signature du rapport d'attestation

Le rapport d'attestation est signé à l'aide d'un certificat, appelé VLEK (Versioned Loaded Endorsement Key), émis par AMD pour AWS. Au cours de cette étape, vous pouvez vérifier que le certificat VLEK est émis par AMD et que le rapport d'attestation est signé par ce certificat VLEK.

1. Téléchargez la racine VLEK des certificats de confiance depuis le site Web officiel d'AMD vers le répertoire actuel.

```
$ C:\> sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/Milan/cert_chain -o ./cert_chain.pem
```

2. Utilisez `openssl` pour vérifier que le certificat VLEK est signé par la racine des certificats de confiance AMD.

```
$ C:\> sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
```

Sortie attendue :

```
certs/vcek.pem: OK
```

3. Utilisez l'utilitaire `snpguest` pour vérifier que le rapport d'attestation est signé par le certificat VLEK.

```
$ C:\> ./snpguest verify attestation ./ report.bin
```

Sortie attendue.

```
Reported TCB Boot Loader from certificate matches the attestation report.  
Reported TCB TEE from certificate matches the attestation report.  
Reported TCB SNP from certificate matches the attestation report.  
Reported TCB Microcode from certificate matches the attestation report.  
VEK signed the Attestation Report!
```

Ajouter des composants du système Windows à l'aide du support d'installation

Les systèmes d'exploitation Windows Server comprennent de nombreux composants facultatifs. L'inclusion de tous les composants facultatifs dans chaque AMI Windows Server Amazon EC2 ne s'avère pas pratique. A la place, nous vous fournissons des instantanés EBS du média d'installation qui ont les fichiers nécessaires pour configurer ou installer des composants sur votre instance Windows.

Pour accéder aux composants facultatifs et les installer, vous devez rechercher l'instantané EBS approprié pour votre version de Windows Server, créer un volume à partir de l'instantané et lier le volume à votre instance.

Avant de commencer

Utilisez l'outil AWS Management Console ou un outil de ligne de commande pour obtenir l'ID d'instance et la zone de disponibilité de votre instance. Vous devez créer un volume EBS dans la même zone de disponibilité que votre instance.

Ajouter des composants Windows à l'aide de la console

Suivez la procédure suivante pour AWS Management Console ajouter des composants Windows à votre instance.

Pour ajouter des composants Windows à une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Dans la barre Filter (Filtre), choisissez Public snapshots (Instantanés publics).
4. Ajoutez le filtre Owner Alias (Alias de propriétaire), puis choisissez amazon.
5. Ajoutez le filtre Description et entrez **Windows**.
6. Appuyez sur Entrée
7. Sélectionnez l'instantané qui correspond à votre architecture système et votre préférence de langue. Par exemple, sélectionnez Windows 2019 English Installation Media si votre instance exécute Windows Server 2019.
8. Choisissez Actions, Create volume from snapshot (Créer un volume à partir d'un instantané).
9. Pour Availability Zone (Zone de disponibilité), sélectionnez la zone de disponibilité correspondant à votre instance Windows. Choisissez Add Tag (Ajouter une identification) et saisissez **Name** pour la clé d'identification et un nom descriptif pour la valeur de la balise. Choisissez Créer un volume.
10. Dans le message Successfully created volume (Volume créé avec succès) (bannière verte), choisissez le volume que vous venez de créer.
11. Sélectionnez Actions, puis Attach volume (Attacher un volume).
12. Depuis Instance, sélectionnez l'ID d'instance.
13. Pour Device name (Nom de périphérique), saisissez le nom du périphérique pour l'attachement. Si vous avez besoin d'aide pour le nom du périphérique, consultez [Noms des appareils sur les instances Amazon EC2](#).
14. Choisissez Attacher un volume.

15. Connectez-vous à votre instance et rendez le volume disponible. Pour plus d'informations, consultez la section [Rendre un volume Amazon EBS disponible pour utilisation](#) dans le guide de l'utilisateur Amazon EBS.

 Important

Ne pas initialiser le volume.

16. Ouvrez le Panneau de configuration, puis Programmes et fonctionnalités. Choisissez Activer ou désactiver des fonctionnalités Windows. Si vous êtes invité à définir un support d'installation, spécifiez le volume EBS avec le support d'installation.
17. (Facultatif) Lorsque vous avez terminé avec le support d'installation, vous pouvez détacher le volume. Après avoir détaché le volume, vous pouvez le supprimer.

Ajouter des composants Windows à l'aide des outils pour Windows PowerShell

Suivez la procédure suivante pour utiliser les Outils pour Windows PowerShell afin d'ajouter des composants Windows à votre instance.

Ajoutez des composants Windows à votre instance à l'aide des outils pour Windows PowerShell

1. Utilisez l'[Get-EC2Snapshot](#) applet de commande avec les description filtres Owner et pour obtenir la liste des instantanés du support d'installation disponibles.

```
PS C:\> Get-EC2Snapshot -Owner amazon -Filter @{ Name="description";  
Values="Windows*" }
```

2. Dans la sortie, notez l'ID de l'instantané qui correspond à votre architecture système et à vos préférences linguistiques. Par exemple :

```
...  
DataEncryptionKeyId :  
Description          : Windows 2019 English Installation Media  
Encrypted            : False  
KmsKeyId             :  
OwnerAlias           : amazon  
OwnerId              : 123456789012  
Progress             : 100%  
SnapshotId          : snap-22da283e  
StartTime            : 10/25/2019 8:00:47 PM
```

```
State           : completed
StateMessage    :
Tags            : {}
VolumeId       : vol-be5eafcb
VolumeSize     : 6
...
```

3. Utilisez l'[New-EC2Volume](#) applet de commande pour créer un volume à partir de l'instantané. Spécifiez la même zone de disponibilité que votre instance.

```
PS C:\> New-EC2Volume -AvailabilityZone us-east-1a -VolumeType gp2 -
SnapshotId snap-22da283e
```

4. Dans la sortie, notez l'ID du volume.

```
Attachments    : {}
AvailabilityZone : us-east-1a
CreateTime     : 4/18/2017 10:50:25 AM
Encrypted      : False
Iops           : 100
KmsKeyId       :
Size           : 6
SnapshotId     : snap-22da283e
State          : creating
Tags           : {}
VolumeId       : vol-06aa9e1fbf8b82ed1
VolumeType     : gp2
```

5. Utilisez l'[Add-EC2Volume](#) applet de commande pour attacher le volume à votre instance.

```
PS C:\> Add-EC2Volume -InstanceId i-087711ddaf98f9489 -
VolumeId vol-06aa9e1fbf8b82ed1 -Device xvdh
```

6. Connectez-vous à votre instance et rendez le volume disponible. Pour plus d'informations, consultez la section [Rendre un volume Amazon EBS disponible pour utilisation](#) dans le guide de l'utilisateur Amazon EBS.

 Important

Ne pas initialiser le volume.

7. Ouvrez le Panneau de configuration, puis Programmes et fonctionnalités. Choisissez Activer ou désactiver des fonctionnalités Windows. Si vous êtes invité à définir un support d'installation, spécifiez le volume EBS avec le support d'installation.
8. (Facultatif) Lorsque vous avez terminé d'utiliser le support d'installation, utilisez l'[Dismount-EC2Volume](#) applet de commande pour détacher le volume de votre instance. Après avoir détaché le volume, vous pouvez utiliser l'[Remove-EC2Volume](#) applet de commande pour le supprimer.

Ajoutez des composants Windows à l'aide du AWS CLI

Suivez la procédure suivante pour AWS CLI ajouter des composants Windows à votre instance.

Pour ajouter des composants Windows à votre instance à l'aide du AWS CLI

1. Utilisez la commande [describe-snapshots](#) avec le paramètre `owner-ids` et le filtre `description` pour obtenir la liste des instantanés de support d'installation disponibles.

```
aws ec2 describe-snapshots --owner-ids amazon --filters
  Name=description,Values=Windows*
```

2. Dans la sortie, notez l'ID de l'instantané qui correspond à votre architecture système et à vos préférences linguistiques. Exemples :

```
{
  "Snapshots": [
    ...
    {
      "OwnerAlias": "amazon",
      "Description": "Windows 2019 English Installation Media",
      "Encrypted": false,
      "VolumeId": "vol-be5eafcb",
      "State": "completed",
      "VolumeSize": 6,
      "Progress": "100%",
      "StartTime": "2019-10-25T20:00:47.000Z",
      "SnapshotId": "snap-22da283e",
      "OwnerId": "123456789012"
    },
    ...
  ]
}
```

3. Utilisez la commande [create-volume](#) pour créer un volume à partir de l'instantané. Spécifiez la même zone de disponibilité que votre instance.

```
aws ec2 create-volume --snapshot-id snap-22da283e --volume-type gp2 --availability-zone us-east-1a
```

4. Dans la sortie, notez l'ID du volume.

```
{
  "AvailabilityZone": "us-east-1a",
  "Encrypted": false,
  "VolumeType": "gp2",
  "VolumeId": "vol-0c98b37f30bcbc290",
  "State": "creating",
  "Iops": 100,
  "SnapshotId": "snap-22da283e",
  "CreateTime": "2017-04-18T10:33:10.940Z",
  "Size": 6
}
```

5. Utilisez la commande [attach-volume](#) pour attacher le volume à votre instance.

```
aws ec2 attach-volume --volume-id vol-0c98b37f30bcbc290 --instance-id i-01474ef662b89480 --device xvdg
```

6. Connectez-vous à votre instance et rendez le volume disponible. Pour plus d'informations, consultez la section [Rendre un volume Amazon EBS disponible pour utilisation](#) dans le guide de l'utilisateur Amazon EBS.

 Important

Ne pas initialiser le volume.

7. Ouvrez le Panneau de configuration, puis Programmes et fonctionnalités. Choisissez Activer ou désactiver des fonctionnalités Windows. Si vous êtes invité à définir un support d'installation, spécifiez le volume EBS avec le support d'installation.
8. (Facultatif) Lorsque vous avez terminé avec le support d'installation, utilisez la commande [detach-volume](#) pour détacher le volume de votre instance. Après avoir détaché le volume, vous pouvez utiliser la commande [delete-volume](#) pour supprimer le volume.

Gérez les utilisateurs du système sur votre instance Linux

Chaque type d'instance Linux est lancé avec un utilisateur du système Linux par défaut. Vous pouvez ajouter et supprimer des utilisateurs de votre instance.

Pour l'utilisateur par défaut, le [nom d'utilisateur par défaut](#) est déterminé par l'AMI qui a été spécifiée au moment du lancement de l'instance.

Note

Par défaut, l'authentification par mot de passe et la connexion racine sont désactivées, et sudo est activé. Pour vous connecter à votre instance, vous devez utiliser une paire de clés. Pour plus d'informations sur la connexion, consultez [Connectez-vous à votre instance Linux](#). Vous pouvez autoriser l'authentification par mot de passe et la connexion racine pour votre instance. Pour plus d'informations, consultez la documentation de votre système d'exploitation.

Note

Les utilisateurs du système Linux ne doivent pas être confondus avec les utilisateurs IAM. Pour plus d'informations, consultez la section [IAM users](#) (Utilisateurs IAM) dans le IAM User Guide (Guide de l'utilisateur IAM).

Table des matières

- [Noms de serveur par défaut](#)
- [Considérations](#)
- [Créer un utilisateur](#)
- [Supprimer un utilisateur](#)

Noms de serveur par défaut

Le nom d'utilisateur par défaut pour votre instance EC2 est déterminé par l'AMI qui a été spécifiée au moment du lancement de l'instance.

Les noms d'utilisateur par défaut sont les suivants :

- Pour AL2023, Amazon Linux 2 ou l'AMI Amazon Linux, le nom d'utilisateur est `ec2-user`.
- Pour une AMI CentOS, le nom d'utilisateur est `centos` ou `ec2-user`.
- Pour une AMI Debian, le nom d'utilisateur est `admin`.
- Pour une AMI Fedora, le nom d'utilisateur est `fedora` ou `ec2-user`.
- Pour une AMI RHEL, le nom d'utilisateur est `root` ou `ec2-user`.
- Pour une AMI SUSE, le nom d'utilisateur est `ec2-user` ou `root`.
- Pour une AMI Ubuntu, le nom utilisateur est `ubuntu`.
- Pour une AMI Oracle, le nom d'utilisateur est `ec2-user`.
- Pour une AMI Bitnami, le nom d'utilisateur est `bitnami`.

Note

Pour trouver le nom d'utilisateur par défaut pour les autres distributions Linux, contactez le fournisseur d'AMI.

Considérations

L'utilisation de l'utilisateur par défaut convient à de nombreuses applications. Toutefois, vous pouvez décider d'ajouter des utilisateurs afin que les individus puissent disposer de leurs propres fichiers et espaces de travail. Par ailleurs, la création d'utilisateurs pour de nouveaux utilisateurs est beaucoup plus sécurisée que l'octroi à plusieurs utilisateurs (probablement inexpérimentés) de l'accès à l'utilisateur par défaut, car l'utilisateur par défaut peut engendrer beaucoup de dommages à un système lorsqu'il est mal utilisé. Pour plus d'informations, consultez [Conseils pour sécuriser votre instance EC2](#).

Pour activer pour les utilisateurs l'accès SSH à votre instance EC2 à l'aide d'un utilisateur du système Linux, vous devez partager la clé SSH avec l'utilisateur. Vous pouvez également utiliser EC2 Instance Connect pour fournir l'accès aux utilisateurs sans devoir partager et gérer les clés SSH. Pour plus d'informations, consultez [Connexion à votre instance Linux avec EC2 Instance Connect](#).

Créez un utilisateur

Créez d'abord l'utilisateur, puis ajoutez la clé publique SSH qui permet à l'utilisateur de se connecter à l'instance.

Pour créer un utilisateur

1. [Créez une nouvelle paire de clés](#). Vous devez fournir le fichier `.pem` à l'utilisateur pour lequel vous créez l'utilisateur. Ils doivent utiliser ce fichier pour se connecter à l'instance.
2. Récupérez la clé publique de la paire de clés que vous avez créée à l'étape précédente.

```
$ C:\> ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
```

La commande renvoie la clé publique, comme indiqué dans l'exemple suivant.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQBAQC1KsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706Vhz2ItxCih
+PnDSUaw+WNQn/mZphTk/a/gU8jEzo0WbkM4yxyb/wB96xbiFveSFJu0p/
d6RJhJ0I0iBxr1sLnBITntckiJ7FbtxJMXLvvwJryDUi1BMTjYtwB+QhYXUM0zce5Pjz5/
i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
+z7wB3RbBQoQzd8v7yeb70z1PnW0yN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

3. Connectez-vous à l'instance.
4. Utilisez la commande `adduser` pour créer l'utilisateur et l'ajouter au système (avec une entrée dans le fichier `/etc/passwd`). Cette commande crée également un groupe et un répertoire de base pour l'utilisateur. Dans cet exemple, l'utilisateur est nommé *newuser*.

- Amazon Linux et Amazon Linux 2

Avec Amazon Linux et Amazon Linux 2, l'utilisateur est créé avec l'authentification par mot de passe désactivée par défaut.

```
[ec2-user ~]$ sudo adduser newuser
```

- Ubuntu

Incluez le paramètre `--disabled-password` pour créer l'utilisateur avec l'authentification par mot de passe désactivée.

```
[ubuntu ~]$ sudo adduser newuser --disabled-password
```

5. Passez au nouvel utilisateur afin que le répertoire et le fichier que vous créez aient le droit de propriété approprié.

```
[ec2-user ~]$ sudo su - newuser
```

L'invite passe de `ec2-user` à `newuser` pour indiquer que vous avez basculé de la session shell au nouvel utilisateur.

6. Ajoutez la clé publique SSH à l'utilisateur. Créez d'abord un répertoire dans le répertoire personnel de l'utilisateur pour le fichier de clé SSH, puis créez le fichier de clé, et enfin collez la clé publique dans le fichier de clé, conformément aux sous-étapes suivantes.
 - a. Créez un répertoire `.ssh` dans le répertoire de base `newuser` et modifiez ses autorisations de fichier en `700` (seul le propriétaire peut ouvrir le répertoire et y lire ou y écrire).

```
[newuser ~]$ mkdir .ssh
```

```
[newuser ~]$ chmod 700 .ssh
```

 Important

Sans les autorisations de fichier exactes, l'utilisateur ne pourra pas se connecter.

- b. Créez un fichier nommé `authorized_keys` dans le répertoire `.ssh` et modifiez ses autorisations de fichier en `600` (seul le propriétaire peut lire le fichier ou y écrire).

```
[newuser ~]$ touch .ssh/authorized_keys
```

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

 Important

Sans les autorisations de fichier exactes, l'utilisateur ne pourra pas se connecter.

- c. Ouvrez le fichier `authorized_keys` avec votre éditeur de texte préféré (comme `vim` ou `nano`).

```
[newuser ~]$ nano .ssh/authorized_keys
```

Collez la clé publique que vous avez récupérée à l'étape 2 dans le fichier et enregistrez les modifications.

⚠ Important

Assurez-vous que vous collez la clé publique dans une ligne continue. La clé publique ne doit pas être divisée sur plusieurs lignes.

L'utilisateur doit pouvoir se connecter à l'utilisateur *newuser* de votre instance à l'aide de la clé privée qui correspond à la clé publique que vous avez ajoutée au fichier `authorized_keys`. Pour plus d'informations sur les différentes méthodes de connexion à une instance Linux, consultez [Connectez-vous à votre instance Linux](#).

Supprimer un utilisateur

Si un utilisateur n'est plus nécessaire, vous pouvez supprimer cet utilisateur pour qu'il ne puisse plus être utilisé.

Utilisez la commande `userdel` pour supprimer l'utilisateur du système. Quand vous spécifiez le paramètre `-r`, le répertoire de base et le fichier temporaire des e-mails de l'utilisateur sont supprimés. Pour conserver le répertoire de base et le fichier temporaire des e-mails de l'utilisateur, omettez le paramètre `-r`.

```
[ec2-user ~]$ sudo userdel -r olduser
```

Définissez le mot de passe d'administrateur Windows pour votre instance

Lorsque vous vous connectez à une instance Windows, vous devez indiquer un compte utilisateur et un mot de passe autorisés à accéder à l'instance. La première fois que vous vous connectez à une instance, un message vous demande de spécifier le compte d'administrateur et le mot de passe par défaut.

Avec les AMI AWS Windows pour Windows Server 2012 R2 et versions antérieures, le mot de passe par défaut est [Configuration d'une instance Windows à l'aide du service EC2Config \(ancien\)](#) généré. Avec les AMI AWS Windows pour Windows Server 2016 et 2019, [Configurer une instance Windows à l'aide d'EC2Launch](#) génère le mot de passe par défaut. Avec les AMI AWS Windows pour Windows

Server 2022 et versions ultérieures, [Configurer une instance Windows à l'aide d'EC2Launch v2](#) génère le mot de passe par défaut.

 Note

Avec Windows Server 2016 ou version ultérieure, l'option `Password never expires` est désactivée pour l'administrateur local. Avec Windows Server 2012 R2 ou version précédente, l'option `Password never expires` est activée par l'administrateur local.

Modifier le mot de passe de l'administrateur après la connexion

Lorsque vous vous connectez à une instance pour la première fois, nous vous recommandons de modifier la valeur entrée par défaut pour le mot de passe administrateur. Procédez comme suit pour modifier le mot de passe Administrateur d'une instance Windows.

 Important

Conservez le nouveau mot de passe en lieu sûr. Vous ne pourrez pas récupérer le nouveau mot de passe à l'aide de la console Amazon EC2. La console ne peut récupérer que le mot de passe par défaut. Si vous tentez de vous connecter à l'instance à l'aide du mot de passe par défaut après l'avoir modifié, vous recevrez l'erreur suivante : « Your credentials did not work » (Vos informations d'identification sont incorrectes).

Pour modifier le mot de passe d'administrateur local

1. Connectez-vous à l'instance et ouvrez une invite de commande.
2. Exécutez la commande suivante. Si votre nouveau mot de passe comporte des caractères spéciaux, vérifiez que vous placez le mot de passe entre guillemets doubles.

```
net user Administrator "new_password"
```

3. Conservez le nouveau mot de passe en lieu sûr.

Modifier un mot de passe perdu ou expiré

Si vous oubliez votre mot de passe ou qu'il expire, vous pouvez générer un nouveau mot de passe. Pour les procédures de réinitialisation de mot de passe, consultez [Réinitialisation d'un mot de passe administrateur Windows perdu ou expiré](#).

Gérez les pilotes de périphériques pour votre instance Amazon EC2

Certains pilotes ne sont pas préinstallés sur l'AMI EC2 à partir de laquelle vous effectuez le lancement. D'autres peuvent avoir besoin de mises à jour afin de bénéficier de fonctionnalités étendues. Les rubriques suivantes traitent de l'installation, des mises à jour et de la configuration de certains pilotes de périphériques associés à vos instances EC2.

Table des matières

- [Installez les pilotes NVIDIA sur votre instance Amazon EC2](#)
- [Installez les pilotes AMD sur votre instance Amazon EC2](#)
- [Pilotes de virtualisation paravirtuelle pour les instances Windows](#)
- [AWS Pilotes NVMe pour instances Windows](#)

Installez les pilotes NVIDIA sur votre instance Amazon EC2

Une instance avec un GPU NVIDIA attaché, telle qu'une instance P3 ou G4dn, doit avoir le pilote NVIDIA approprié installé. En fonction du type d'instance, vous pouvez télécharger un pilote NVIDIA public, télécharger un pilote depuis Amazon Simple Storage (Amazon S3) disponible uniquement pour les clients AWS ou utiliser une AMI avec le pilote préinstallé.

Pour installer les pilotes AMD sur une instance à laquelle est connecté un GPU AMD, telle qu'une instance G4ad, consultez [Installer les pilotes AMD](#). Pour installer les pilotes NVIDIA, consultez [Installer les pilotes NVIDIA](#).

Table des matières

- [Types de pilote NVIDIA](#)
- [Pilotes disponibles par type d'instance](#)
- [Options d'installation](#)

- [Option 1 : AMI avec les pilotes NVIDIA installés](#)
- [Option 2 : Pilotes NVIDIA publics](#)
- [Option 3 : pilotes GRID \(instances G6, Gr6, G5, G4dn et G3\)](#)
- [Option 4 : pilotes de jeu NVIDIA \(instances G4dn et G5\)](#)
- [Installer une version supplémentaire de CUDA](#)

Types de pilote NVIDIA

Voici les principaux types de pilote NVIDIA qui peuvent être utilisés avec des instances basées sur GPU.

Pilotes Tesla

Ces pilotes sont principalement destinés aux charges de travail de calcul, qui utilisent des GPU pour des tâches de calcul telles que les calculs parallélisés à virgule flottante pour le machine learning et les transformations de Fourier rapides pour les applications de calcul hautes performances.

Pilotes GRID

Ces pilotes sont certifiés pour fournir des performances optimales pour les applications de visualisation professionnelles qui traitent des contenus tels que des modèles 3D ou des vidéos haute résolution. Vous pouvez configurer les pilotes GRID pour prendre en charge deux modes. Les stations de travail virtuelles Quadro permettent d'accéder à quatre écrans 4K par GPU. Les vApps GRID fournissent des fonctionnalités d'hébergement RDSH App.

Pilotes de jeu

Ces pilotes contiennent des optimisations pour le jeu et sont fréquemment mis à jour pour améliorer les performances. Ils prennent en charge un seul écran 4K par GPU.

Mode configuré

Sous Windows, les pilotes Tesla sont configurés pour s'exécuter en mode Tesla Compute Cluster (TCC). Les pilotes GRID et de jeu sont configurés pour s'exécuter en mode WDDM (Windows Display Driver Model). En mode TCC, la carte est dédiée aux charges de travail de calcul. En mode WDDM, la carte prend en charge les charges de travail de calcul et les charges de travail graphiques.

Panneau de configuration NVIDIA

Le panneau de commande NVIDIA est pris en charge avec les pilotes GRID et Gaming. Il n'est pas pris en charge avec les pilotes Tesla.

API prises en charge pour les pilotes Tesla, GRID et gaming

- OpenCL, OpenGL et Vulkan
- NVIDIA CUDA et bibliothèques associées (par exemple, cuDNN, TensorRT, nvJPEG et cuBLAS)
- NVENC pour l'encodage vidéo et NVDEC pour le décodage vidéo
- API réservées à Windows : DirectX, Direct2D, Accélération vidéo DirectX, Raytracing DirectX

Pilotes disponibles par type d'instance

Le tableau suivant récapitule les pilotes NVIDIA pris en charge pour chaque type d'instance de GPU.

Type d'instance	Pilote Tesla	Pilote GRID	Pilote de jeu
G3	Oui	Oui	Non
G4dn	Oui	Oui	Oui
G5	Oui	Oui	Oui
G5g	Oui ¹	Non	Non
G6	Oui	Oui	Non
Gr 6	Oui	Oui	Non
P2	Oui	Non	Non
P3	Oui	Non	Non
P4d	Oui	Non	Non
P4de	Oui	Non	Non

¹ Ce pilote Tesla prend également en charge les applications graphiques optimisées spécifiques à la plateforme ARM64

² Utilisation d'AMI Marketplace uniquement

Options d'installation

Utilisez l'une des options suivantes pour obtenir les pilotes NVIDIA requis pour votre instance de GPU.

Options

- [Option 1 : AMI avec les pilotes NVIDIA installés](#)
- [Option 2 : Pilotes NVIDIA publics](#)
- [Option 3 : pilotes GRID \(instances G6, Gr6, G5, G4dn et G3\)](#)
- [Option 4 : pilotes de jeu NVIDIA \(instances G4dn et G5\)](#)

Option 1 : AMI avec les pilotes NVIDIA installés

AWS et NVIDIA proposent différentes Amazon Machine Images (AMI) fournies avec les pilotes NVIDIA installés.

- [Offres Marketplace avec le pilote Tesla](#)
- [Offres Marketplace avec le pilote GRID](#)
- [Offres Marketplace avec le pilote de jeu](#)

Pour passer en revue les considérations qui dépendent de la plate-forme de votre système d'exploitation (OS), choisissez l'onglet qui s'applique à votre AMI.

Linux

Pour mettre à jour la version du pilote installée à l'aide de l'une de ces AMI, vous devez désinstaller les packages NVIDIA de votre instance pour éviter les conflits de version. Utilisez cette commande pour désinstaller les packages NVIDIA :

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

Le package de boîte à outils CUDA fourni par Amazon comporte des dépendances sur les pilotes NVIDIA. La désinstallation des packages NVIDIA efface la boîte à outils CUDA. Vous devez réinstaller la boîte à outils CUDA après avoir installé le pilote NVIDIA.

Windows

Si vous créez une AMI Windows personnalisée à l'aide de l'une des AWS Marketplace offres, l'AMI doit être une image standardisée créée avec Windows Sysprep pour garantir le fonctionnement du pilote GRID. Pour plus d'informations, consultez [Création d'une AMI avec Windows Sysprep](#).

Option 2 : Pilotes NVIDIA publics

Les options proposées AWS sont accompagnées du permis nécessaire pour le conducteur. Alternativement, vous pouvez installer les pilotes publics et apporter votre propre licence. Pour installer un pilote public, téléchargez-le à partir du site NVIDIA comme décrit ici.

Vous pouvez également utiliser les options proposées par les conducteurs publics à la AWS place. Pour utiliser un pilote GRID sur une instance P3, utilisez les AWS Marketplace AMI comme décrit dans [l'option 1](#). Pour utiliser un pilote GRID sur une instance G6, Gr6, G5, G4dn ou G3, utilisez les AWS Marketplace AMI comme décrit dans l'option 1 ou installez les pilotes NVIDIA fournis par comme décrit dans. AWS [Option 3 : pilotes GRID \(instances G6, Gr6, G5, G4dn et G3\)](#)

Pour télécharger un pilote NVIDIA public

Connectez-vous à votre instance et téléchargez le pilote NVIDIA 64 bits adapté au type d'instance depuis <http://www.nvidia.com/Download/Find.aspx>. Pour Type de produit, Série de produits et Produit, utilisez les options du tableau suivant.

Instance	Type de produit	Série de produits	Produit
G3	Tesla	M-Class	M60
G4dn	Tesla	T-Series	T4
G5 ¹	Tesla	Série A	A10
G5g ²	Tesla	T-Series	NVIDIA T4G
G6 ³	Tesla	Série L	L4
Gr 6 ³	Tesla	Série L	L4
P2	Tesla	Série K	K80

Instance	Type de produit	Série de produits	Produit
P3	Tesla	Série V	V100
P4d	Tesla	Série A	A100
P4de	Tesla	Série A	A100
P5 (4)	Tesla	Série H	H100

¹ Les instances G5 ont besoin d'un pilote de version 470.00 ou ultérieure

² Les instances G5g ont besoin d'un pilote de version 470.82.01 ou ultérieure. Le système d'exploitation est Linux aarch64

³ Les instances G6 et Gr6 nécessitent la version du pilote 525.0 ou ultérieure.

⁴ instances P5 nécessitent la version 530 ou ultérieure du pilote.

Pour installer le pilote NVIDIA sur les systèmes d'exploitation Linux, consultez le [guide de démarrage rapide d'installation du pilote NVIDIA](#).

Pour installer le pilote NVIDIA sous Windows, procédez comme suit :

1. Ouvrez le dossier dans lequel vous avez téléchargé le pilote et lancez le fichier d'installation. Suivez les instructions pour installer le pilote et redémarrez votre instance le cas échéant.
2. Désactivez la carte vidéo nommée Microsoft Basic Display Adapter qui est marquée d'une icône d'avertissement à l'aide du Gestionnaire de périphériques. Installez les fonctionnalités Windows : Media Foundation et Quality Windows Audio Video Experience.

 Important

Ne désactivez pas la carte vidéo nommée Microsoft Remote Display Adapter. Si Microsoft Remote Display Adapter est désactivée, votre connexion peut s'interrompre et les tentatives de connexion à l'instance après son redémarrage peuvent échouer.

3. Pour vous assurer que le GPU fonctionne correctement, vérifiez le Gestionnaire de périphériques.

4. Effectuez les étapes d'optimisation de [Optimisation des paramètres GPU sur les instances Amazon EC2](#) pour bénéficier des meilleures performances de votre GPU.

Option 3 : pilotes GRID (instances G6, Gr6, G5, G4dn et G3)

Ces téléchargements ne sont disponibles que pour AWS les clients. En téléchargeant, afin de respecter les exigences de la AWS solution mentionnées dans le contrat de licence utilisateur final (EULA) NVIDIA GRID Cloud, vous acceptez d'utiliser le logiciel téléchargé uniquement pour développer des AMI destinées à être utilisées avec le matériel NVIDIA L4, NVIDIA A10G, NVIDIA Tesla T4 ou NVIDIA Tesla M60. Dès l'installation du logiciel, vous êtes lié par les conditions du document [Contrat de licence utilisateur final NVIDIA GRID Cloud](#). Pour plus d'informations sur la version du pilote NVIDIA GRID adaptée à votre système d'exploitation, veuillez consulter la [documentation du logiciel NVIDIA® de GPU virtuel \(vGPU\)](#) sur le site Web de NVIDIA.

Considérations

- Les instances G6 et Gr6 nécessitent GRID 17 ou version ultérieure.
- Les instances G5 nécessitent GRID 13.1 ou version ultérieure (ou GRID 12.4 ou version ultérieure).
- Les instances G3 nécessitent une résolution DNS AWS fournie pour que les licences GRID fonctionnent.
- [IMDSv2](#) n'est pris en charge qu'avec le pilote NVIDIA version 14.0 ou supérieure.
- Pour les instances Windows, si vous lancez votre instance à partir d'une AMI Windows personnalisée, l'AMI doit être une image standardisée créée avec Windows Sysprep pour garantir le fonctionnement du pilote GRID. Pour plus d'informations, consultez [Création d'une AMI avec Windows Sysprep](#).
- GRID 17.0 et versions ultérieures ne sont pas compatibles avec Windows Server 2019.
- GRID 14.2 et versions ultérieures ne sont pas compatibles avec Windows Server 2016.
- GRID 17.0 et versions ultérieures ne sont pas pris en charge avec les instances G3.

Amazon Linux et Amazon Linux 2

Pour installer le pilote NVIDIA GRID sur votre instance

1. Connectez-vous à votre instance Linux.

2. Installez-le AWS CLI sur votre instance Linux et configurez les informations d'identification par défaut. Pour plus d'informations, consultez [Installation d' AWS CLI](#) dans le Guide de l'utilisateur AWS Command Line Interface .

⚠ Important

Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'ReadOnlyaccès d'AmazonS3. Pour plus d'informations, consultez la [politique AWS gérée : AmazonS3 ReadOnly Access](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

3. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo yum install gcc make
```

4. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

5. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

6. Reconnectez-vous à votre instance après son redémarrage.
7. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

8. Téléchargez l'utilitaire d'installation du pilote GRID à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Plusieurs versions du pilote GRID sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Exécutez le script d'auto-installation comme suit pour installer le pilote GRID que vous avez téléchargé. Par exemple :

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Note

Si vous utilisez Amazon Linux 2 avec le noyau version 5.10, utilisez la commande suivante pour installer le pilote GRID.

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

11. Vérifiez que le pilote fonctionne. La sortie de la commande suivante affiche la version installée du pilote NVIDIA, ainsi que des détails sur les GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

12. Si vous utilisez le logiciel vGPU NVIDIA version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

14. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.
 - a. (Facultatif) Pour profiter des quatre écrans d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#).
 - b. Le mode de station de travail virtuelle NVIDIA Quadro est activé par défaut. Pour activer les fonctionnalités d'hébergement de GRID Virtual Applications for RDSH Application, suivez les étapes d'activation de GRID Virtual Applications dans [Activez les applications virtuelles NVIDIA GRID sur vos instances basées sur le GPU Amazon EC2](#).

CentOS 7 et Red Hat Enterprise Linux 7

Pour installer le pilote NVIDIA GRID sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.
2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

6. Désactivez le pilote nouveau open source pour les cartes graphiques NVIDIA.
 - a. Ajoutez nouveau au fichier de liste noire `/etc/modprobe.d/blacklist.conf`. Copiez le bloc de code suivant et collez-le dans un terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
```

```
blacklist nvidiafb
blacklist rivatv
EOF
```

- b. Modifiez le fichier `/etc/default/grub` et ajoutez la ligne suivante :

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- c. Générez à nouveau la configuration Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Téléchargez l'utilitaire d'installation du pilote GRID à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Plusieurs versions du pilote GRID sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. Exécutez le script d'auto-installation comme suit pour installer le pilote GRID que vous avez téléchargé. Exemples :

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

10. Vérifiez que le pilote fonctionne. La sortie de la commande suivante affiche la version installée du pilote NVIDIA, ainsi que des détails sur les GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. Si vous utilisez le logiciel vGPU NVIDIA version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

12. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

13. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

- a. (Facultatif) Pour profiter des quatre écrans d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#).
- b. Le mode de station de travail virtuelle NVIDIA Quadro est activé par défaut. Pour activer les fonctionnalités d'hébergement de GRID Virtual Applications for RDSH Application, suivez les étapes d'activation de GRID Virtual Applications dans [Activez les applications virtuelles NVIDIA GRID sur vos instances basées sur le GPU Amazon EC2](#).
- c. Installez le package de poste de travail de l'interface graphique.

```
[ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
```

CentOS Stream 8 et Red Hat Enterprise Linux 8

Pour installer le pilote NVIDIA GRID sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.
2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel kernel-devel-$(uname -r)
```

6. Téléchargez l'utilitaire d'installation du pilote GRID à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Plusieurs versions du pilote GRID sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Exécutez le script d'auto-installation comme suit pour installer le pilote GRID que vous avez téléchargé. Exemples :

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

9. Vérifiez que le pilote fonctionne. La sortie de la commande suivante affiche la version installée du pilote NVIDIA, ainsi que des détails sur les GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Si vous utilisez le logiciel vGPU NVIDIA version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /  
etc/modprobe.d/nvidia.conf
```

11. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

12. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

- a. (Facultatif) Pour profiter des quatre écrans d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#).
- b. Le mode de station de travail virtuelle NVIDIA Quadro est activé par défaut. Pour activer les fonctionnalités d'hébergement de GRID Virtual Applications for RDSH Application, suivez les étapes d'activation de GRID Virtual Applications dans [Activez les applications virtuelles NVIDIA GRID sur vos instances basées sur le GPU Amazon EC2](#).
- c. Installez le package de poste de travail de l'interface graphique.

```
[ec2-user ~]$ sudo dnf groupinstall -y workstation
```

Rocky Linux 8

Pour installer le pilote NVIDIA GRID sur votre instance Linux

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.
2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.

5. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel kernel-devel-$(uname -r)
```

6. Téléchargez l'utilitaire d'installation du pilote GRID à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Plusieurs versions du pilote GRID sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Exécutez le script d'auto-installation comme suit pour installer le pilote GRID que vous avez téléchargé. Exemples :

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

9. Vérifiez que le pilote fonctionne. La sortie de la commande suivante affiche la version installée du pilote NVIDIA, ainsi que des détails sur les GPU.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Si vous utilisez le logiciel vGPU NVIDIA version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

11. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

12. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

- a. (Facultatif) Pour profiter des quatre écrans d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#).
- b. Le mode de station de travail virtuelle NVIDIA Quadro est activé par défaut. Pour activer les fonctionnalités d'hébergement de GRID Virtual Applications for RDSH Application, suivez les étapes d'activation de GRID Virtual Applications dans [Activez les applications virtuelles NVIDIA GRID sur vos instances basées sur le GPU Amazon EC2](#).

Ubuntu et Debian

Pour installer le pilote NVIDIA GRID sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.
2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
$ sudo apt-get update -y
```

3. (Ubuntu) Mettez à niveau le package `linux-aws` pour recevoir la version la plus récente.

```
$ sudo apt-get upgrade -y linux-aws
```

(Debian) Mettez à niveau le package pour recevoir la version la plus récente.

```
$ sudo apt-get upgrade -y
```

4. Redémarrez votre instance pour charger la dernière version du noyau.

```
$ sudo reboot
```

5. Reconnectez-vous à votre instance après son redémarrage.
6. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

7. Désactivez le pilote nouveau open source pour les cartes graphiques NVIDIA.
 - a. Ajoutez nouveau au fichier de liste noire `/etc/modprobe.d/blacklist.conf`. Copiez le bloc de code suivant et collez-le dans un terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- b. Modifiez le fichier `/etc/default/grub` et ajoutez la ligne suivante :

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- c. Générez à nouveau la configuration Grub.

```
$ sudo update-grub
```

8. Téléchargez l'utilitaire d'installation du pilote GRID à l'aide de la commande suivante :

```
$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Plusieurs versions du pilote GRID sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante.

```
$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante.

```
$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Exécutez le script d'auto-installation comme suit pour installer le pilote GRID que vous avez téléchargé. Exemples :

```
$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

11. Vérifiez que le pilote fonctionne. La sortie de la commande suivante affiche la version installée du pilote NVIDIA, ainsi que des détails sur les GPU.

```
$ nvidia-smi -q | head
```

12. Si vous utilisez le logiciel vGPU NVIDIA version 14.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Redémarrez l'instance.

```
$ sudo reboot
```

14. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

- a. (Facultatif) Pour profiter des quatre écrans d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#).
- b. Le mode de station de travail virtuelle NVIDIA Quadro est activé par défaut. Pour activer les fonctionnalités d'hébergement de GRID Virtual Applications for RDSH Application, suivez les étapes d'activation de GRID Virtual Applications dans [Activez les applications virtuelles NVIDIA GRID sur vos instances basées sur le GPU Amazon EC2](#).
- c. Installez le package de poste de travail de l'interface graphique.

```
$ sudo apt-get install -y lightdm ubuntu-desktop
```

Systèmes d'exploitation Windows

Pour installer le pilote NVIDIA GRID sur votre instance Windows

1. Connectez-vous à votre instance Windows et ouvrez une PowerShell fenêtre.
2. Configurez les informations d'identification par défaut pour votre instance Windows. AWS Tools for Windows PowerShell Pour plus d'informations, voir [Démarrer avec les AWS Tools for Windows PowerShell](#) dans le Guide de l'utilisateur AWS Tools for Windows PowerShell .

Important

Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'ReadOnlyaccès d'AmazonS3. Pour plus d'informations, consultez la [politique AWS gérée : AmazonS3 ReadOnly Access](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

3. Téléchargez les pilotes et le [contrat de licence utilisateur final NVIDIA GRID Cloud](#) depuis Amazon S3 sur votre bureau à l'aide des PowerShell commandes suivantes.

```
$Bucket = "ec2-windows-nvidia-drivers"
$KeyPrefix = "latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
    $LocalFileName = $Object.Key
    if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
        $LocalFilePath = Join-Path $LocalPath $LocalFileName
        Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
    }
}
```

Plusieurs versions du pilote NVIDIA GRID sont stockées dans ce compartiment. Vous pouvez télécharger toutes les versions Windows disponibles dans le compartiment en supprimant l'option `-KeyPrefix $KeyPrefix`. Pour plus d'informations sur la version du pilote NVIDIA GRID adaptée à votre système d'exploitation, veuillez consulter la [documentation du logiciel NVIDIA® de GPU virtuel \(vGPU\)](#) sur le site Web de NVIDIA.

À partir de GRID version 11.0, vous pouvez utiliser les pilotes sous `latest` pour les instances G3 et G4dn. Nous n'ajouterons pas les versions postérieures à 11.0 à `g4/latest`, mais nous conserverons la version 11.0 et les versions antérieures spécifiques à G4dn sous `g4/latest`.

Les instances G5 nécessitent GRID 13.1 ou version ultérieure (ou GRID 12.4 ou version ultérieure).

4. Accédez au bureau et double-cliquez sur le fichier d'installation pour le lancer (choisissez la version du pilote qui correspond à la version du système d'exploitation de votre instance). Suivez les instructions pour installer le pilote et redémarrez votre instance le cas échéant. Pour vous assurer que le GPU fonctionne correctement, vérifiez le Gestionnaire de périphériques.
5. (Facultatif) Utilisez la commande suivante pour désactiver la page des licences dans le panneau de configuration pour empêcher les utilisateurs de modifier accidentellement le type de produit (la station de travail virtuelle NVIDIA GRID est activée par défaut). Pour plus d'informations, consultez le manuel [GRID Licensing User Guide](#).

PowerShell

Exécutez les PowerShell commandes suivantes pour créer la valeur de registre afin de désactiver la page de licence dans le panneau de configuration. Les AMI AWS Tools for PowerShell de AWS Windows utilisent par défaut la version 32 bits et cette commande échoue. Utilisez plutôt la version 64 bits PowerShell fournie avec le système d'exploitation.

```
New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing  
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -  
Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
```

Invite de commande

Exécutez la commande de registre suivante pour créer la valeur de registre afin de désactiver la page des licences dans le panneau de configuration. Vous pouvez l'exécuter à l'aide de la fenêtre d'invite de commandes ou d'une version 64 bits de PowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v  
NvCplDisableManageLicensePage /t REG_DWORD /d 1
```

6. (Facultatif) Selon votre cas d'utilisation, vous pouvez effectuer les étapes facultatives suivantes. Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas ces étapes.

- a. Pour profiter des quatre écrans d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance, [NICE DCV](#).
- b. Le mode de station de travail virtuelle NVIDIA Quadro est activé par défaut. Pour activer les fonctionnalités d'hébergement de GRID Virtual Applications for RDSH Application, suivez les étapes d'activation de GRID Virtual Applications dans [Activez les applications virtuelles NVIDIA GRID sur vos instances basées sur le GPU Amazon EC2](#).

Option 4 : pilotes de jeu NVIDIA (instances G4dn et G5)

Ces pilotes ne sont disponibles que pour AWS les clients. En les téléchargeant, vous acceptez de n'utiliser le logiciel téléchargé que pour développer des AMI destinées à être utilisées avec le matériel NVIDIA A10G et NVIDIA Tesla T4. Dès l'installation du logiciel, vous êtes lié par les conditions du document [Contrat de licence utilisateur final NVIDIA GRID Cloud](#).

Considérations

- Les instances G3 nécessitent une résolution DNS AWS fournie pour que les licences GRID fonctionnent.
- [IMDSv2](#) n'est pris en charge qu'avec le pilote NVIDIA version 495.x ou supérieure.

Amazon Linux et Amazon Linux 2

Pour installer le pilote de jeu NVIDIA sur votre instance

1. Connectez-vous à votre instance Linux.
2. Installez-le AWS CLI sur votre instance Linux et configurez les informations d'identification par défaut. Pour plus d'informations, consultez [Installation d' AWS CLI](#) dans le Guide de l'utilisateur AWS Command Line Interface .

Important

Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'ReadOnlyaccès d'AmazonS3. Pour plus d'informations, consultez la [politique AWS gérée : AmazonS3 ReadOnly Access](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

3. Installez gcc et make, si ce n'est pas déjà fait.

```
[ec2-user ~]$ sudo yum install gcc make
```

4. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

5. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

6. Reconnectez-vous à votre instance après son redémarrage.
7. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

8. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé .zip.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

10. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

11. Exécutez le programme d'installation à l'aide de la commande suivante :

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Note

Si vous utilisez Amazon Linux 2 avec le noyau version 5.10, utilisez la commande suivante pour installer les pilotes de jeu NVIDIA.

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

12. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.

- Pour la version 460.39 ou ultérieure :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

- Pour les versions 440.68 à 445.48 :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Pour des versions antérieures :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Si vous utilisez le pilote NVIDIA version 510.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

15. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

16. (Facultatif) Pour profiter d'un seul écran d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#).

CentOS 7 et Red Hat Enterprise Linux 7

Pour installer le pilote de jeu NVIDIA sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.
2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. Désactivez le pilote nouveau open source pour les cartes graphiques NVIDIA.
 - a. Ajoutez nouveau au fichier de liste noire `/etc/modprobe.d/blacklist.conf`. Copiez le bloc de code suivant et collez-le dans un terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
```

```
blacklist nvidiafb
blacklist rivatv
EOF
```

- b. Modifiez le fichier `/etc/default/grub` et ajoutez la ligne suivante :

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- c. Générez à nouveau la configuration Grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé `.zip`.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

10. Exécutez le programme d'installation à l'aide de la commande suivante :

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

11. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
```

EOF

12. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.

- Pour la version 460.39 ou ultérieure :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

- Pour les versions 440.68 à 445.48 :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Pour des versions antérieures :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Si vous utilisez le pilote NVIDIA version 510.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

14. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

15. (Facultatif) Pour profiter d'un seul écran d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#). Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas cette étape.

CentOS Stream 8 et Red Hat Enterprise Linux 8

Pour installer le pilote de jeu NVIDIA sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.

2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé .zip.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Exécutez le programme d'installation à l'aide de la commande suivante :

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

10. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.

- Pour la version 460.39 ou ultérieure :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

- Pour les versions 440.68 à 445.48 :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Pour des versions antérieures :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Si vous utilisez le pilote NVIDIA version 510.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

14. (Facultatif) Pour profiter d'un seul écran d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#).

Rocky Linux 8

Pour installer le pilote de jeu NVIDIA sur votre instance

1. Connectez-vous à votre instance Linux. Installez gcc et make, si ce n'est pas déjà fait.
2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
[ec2-user ~]$ sudo yum update -y
```

3. Redémarrez votre instance pour charger la dernière version du noyau.

```
[ec2-user ~]$ sudo reboot
```

4. Reconnectez-vous à votre instance après son redémarrage.
5. Installez le compilateur gcc et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
[ec2-user ~]$ sudo dnf install -y unzip gcc make elfutils-libelf-devel libglvnd-devel kernel-devel-$(uname -r)
```

6. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé .zip.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Exécutez le programme d'installation à l'aide de la commande suivante :

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

10. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.

- Pour la version 460.39 ou ultérieure :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

- Pour les versions 440.68 à 445.48 :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Pour des versions antérieures :

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Si vous utilisez le pilote NVIDIA version 510.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Redémarrez l'instance.

```
[ec2-user ~]$ sudo reboot
```

14. (Facultatif) Pour profiter d'un seul écran d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#).

Ubuntu et Debian

Pour installer le pilote de jeu NVIDIA sur votre instance

1. Connectez-vous à votre instance Linux. Installez `gcc` et `make`, si ce n'est pas déjà fait.
2. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

```
$ sudo apt-get update -y
```

3. Mettez à niveau le package `linux-aws` pour recevoir la version la plus récente.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Redémarrez votre instance pour charger la dernière version du noyau.

```
$ sudo reboot
```

5. Reconnectez-vous à votre instance après son redémarrage.
6. Installez le compilateur `gcc` et le package d'en-têtes de noyau correspondant à la version du noyau que vous utilisez actuellement.

```
$ sudo apt-get install -y unzip gcc make linux-headers-$(uname -r)
```

7. Désactivez le pilote nouveau open source pour les cartes graphiques NVIDIA.
 - a. Ajoutez nouveau au fichier de liste noire `/etc/modprobe.d/blacklist.conf`. Copiez le bloc de code suivant et collez-le dans un terminal.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- b. Modifiez le fichier `/etc/default/grub` et ajoutez la ligne suivante :

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- c. Générez à nouveau la configuration Grub.

```
$ sudo update-grub
```

8. Téléchargez l'utilitaire d'installation du pilote de jeu à l'aide de la commande suivante :

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Plusieurs versions du pilote de jeu sont stockées dans ce compartiment. Vous pouvez voir toutes les versions disponibles à l'aide de la commande suivante :

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extrayez l'utilitaire d'installation du pilote de jeu de l'archive téléchargé `.zip`.

```
$ unzip vGPUW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Ajoutez les autorisations pour exécuter l'utilitaire d'installation du pilote à l'aide de la commande suivante :

```
$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

11. Exécutez le programme d'installation à l'aide de la commande suivante :

```
$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Lorsque vous y êtes invité, acceptez le contrat de licence et spécifiez les options d'installation comme requis (vous pouvez accepter les options par défaut).

12. Utilisez la commande suivante pour créer le fichier de configuration requis.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Utilisez la commande suivante pour télécharger et renommer le fichier de certification.

- Pour la version 460.39 ou ultérieure :

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

- Pour les versions 440.68 à 445.48 :

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Pour des versions antérieures :

```
$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

14. Si vous utilisez le pilote NVIDIA version 510.x ou supérieure sur les instances G4dn, G5 ou G5g, désactivez GSP avec les commandes suivantes. Pour plus d'informations sur les raisons de cette exigence, consultez la [Documentation NVIDIA](#).

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

15. Redémarrez l'instance.

```
$ sudo reboot
```

16. (Facultatif) Pour profiter d'un seul écran d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#). Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas cette étape.

Systèmes d'exploitation Windows

Avant d'installer un pilote de jeu NVIDIA sur votre instance, vous devez vous assurer que les conditions préalables suivantes sont remplies, en plus des considérations mentionnées pour tous les pilotes de jeu.

- Si vous lancez votre instance Windows à l'aide d'une AMI Windows personnalisée, l'AMI doit être une image standardisée créée avec Windows Sysprep pour garantir le fonctionnement du pilote de jeu. Pour plus d'informations, consultez [Création d'une AMI avec Windows Sysprep](#).
- Configurez les informations d'identification par défaut pour votre instance Windows. AWS Tools for Windows PowerShell Pour plus d'informations, voir [Démarrer avec les AWS Tools for Windows PowerShell](#) dans le Guide de l'utilisateur AWS Tools for Windows PowerShell .
- Vos utilisateurs ou votre rôle doivent disposer des autorisations accordées conformément à la politique d'ReadOnlyaccès d'AmazonS3. Pour plus d'informations, consultez la [politique AWS gérée : AmazonS3 ReadOnly Access](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour installer le pilote de jeu NVIDIA sur votre instance Windows

1. Connectez-vous à votre instance Windows et ouvrez une PowerShell fenêtre.
2. Téléchargez et installez le pilote de jeu à l'aide des PowerShell commandes suivantes.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
    $LocalFileName = $Object.Key
    if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
        $LocalFilePath = Join-Path $LocalPath $LocalFileName
        Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
    }
}
```

Plusieurs versions du pilote NVIDIA GRID sont stockées dans ce compartiment S3. Vous pouvez télécharger toutes les versions disponibles dans le compartiment si vous modifiez la valeur de la `$KeyPrefix` variable de "windows/latest" à "windows".

3. Accédez au bureau et double-cliquez sur le fichier d'installation pour le lancer (choisissez la version du pilote qui correspond à la version du système d'exploitation de votre instance). Suivez les instructions pour installer le pilote et redémarrez votre instance le cas échéant. Pour vous assurer que le GPU fonctionne correctement, consultez le Gestionnaire de périphériques.
4. Utilisez l'une des méthodes suivantes pour enregistrer le pilote.

Version 527.27 or above

Créez la clé de registre suivante à l'aide de la version 64 bits de PowerShell ou de la fenêtre d'invite de commande.

Clé : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global

nom : vGamingMarketplace

type : DWord

valeur : 2

PowerShell

Exécutez la PowerShell commande suivante pour créer cette valeur de registre. Les AMI AWS Tools for PowerShell de AWS Windows utilisent par défaut la version 32 bits et cette commande échoue. Utilisez plutôt la version 64 bits PowerShell fournie avec le système d'exploitation.

```
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
-Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Invite de commande

Exécutez la commande de registre suivante pour créer cette valeur de registre. Vous pouvez l'exécuter à l'aide de la fenêtre d'invite de commandes ou d'une version 64 bits de PowerShell.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
vGamingMarketplace /t REG_DWORD /d 2
```

Earlier versions

Créez la clé de registre suivante à l'aide de la version 64 bits de PowerShell ou de la fenêtre d'invite de commande.

Clé : HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global

nom : vGamingMarketplace

type : DWord

valeur : 2

PowerShell

Exécutez la PowerShell commande suivante pour créer cette valeur de registre. Les AMI AWS Tools for PowerShell de AWS Windows utilisent par défaut la version 32 bits et cette commande échoue. Utilisez plutôt la version 64 bits PowerShell fournie avec le système d'exploitation.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name  
"vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Invite de commande

Exécutez la commande de registre suivante pour créer cette clé de registre avec la fenêtre d'invite de commandes. Vous pouvez également utiliser cette commande dans la version 64 bits de PowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t  
REG_DWORD /d 2
```

5. Exécutez la commande suivante dans PowerShell. Celle-ci télécharge le fichier de certification, le renomme en `GridSwCert.txt` et le déplace vers le dossier Public Documents (Documents publics) sur votre lecteur système. En général, le chemin du dossier est `C:\Users\Public\Documents`.

- Pour la version 461.40 ou ultérieure :

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-  
Archive/GridSwCertWindows_2023_9_22.cert" -OutFile "$Env:PUBLIC\Documents  
\GridSwCert.txt"
```

- Pour la version 445.87 :

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents\nvidia-cert.txt"
```

- Pour des versions antérieures :

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents\nvidia-cert.txt"
```

Note

Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que le protocole TLS 1.2 doive être activé sur votre PowerShell terminal. Vous pouvez activer le protocole TLS 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol =  
[Net.SecurityProtocolType]::Tls12
```

6. Redémarrez votre instance.
7. Vérifiez la licence de jeu NVIDIA à l'aide de la commande suivante.

```
C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\nvidia-smi.exe -q
```

La sortie doit ressembler à ce qui suit.

```
vGPU Software Licensed Product  
Product Name           : NVIDIA Cloud Gaming  
License Status         : Licensed (Expiry: N/A)
```

8. (Facultatif) Pour profiter d'un seul écran d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance [NICE DCV](#). Si vous n'avez pas besoin de cette fonctionnalité, n'effectuez pas cette étape.

Installer une version supplémentaire de CUDA

Après avoir installé un pilote graphique NVIDIA sur votre instance, vous pouvez installer une version de CUDA autre que celle fournie avec le pilote graphique. La procédure suivante montre comment configurer plusieurs versions de CUDA sur l'instance.

Installez le kit d'outils CUDA sous Linux

Suivez ces étapes pour installer le kit d'outils CUDA sous Linux :

1. Connectez-vous à votre instance Linux.
2. Ouvrez le [site web NVIDIA](#) et sélectionnez la version de CUDA dont vous avez besoin.
3. Sélectionnez l'architecture, la distribution et la version du système d'exploitation de votre instance. Pour Installer Type (Type de programme d'installation), sélectionnez runfile (local).
4. Suivez les instructions pour télécharger le script d'installation.
5. Ajoutez les autorisations d'exécution au script d'installation que vous avez téléchargé à l'aide de la commande suivante.

```
[ec2-user ~]$ chmod +x downloaded_installer_file
```

6. Exécutez le script d'installation comme suit pour installer la boîte à outils CUDA et ajouter le numéro de version CUDA au chemin d'accès de la boîte à outils.

```
[ec2-user ~]$ sudo sh downloaded_installer_file --silent --override --toolkit --samples --toolkitpath=/usr/local/cuda-version --samplespath=/usr/local/cuda --no-opengl-libs
```

7. (Facultatif) Définissez la version CUDA par défaut comme suit.

```
[ec2-user ~]$ sudo ln -s /usr/local/cuda-version /usr/local/cuda
```

Installez le kit d'outils CUDA sous Windows

Procédez comme suit pour installer le kit d'outils CUDA sous Windows :

Pour installer la boîte à outils CUDA

1. Connectez-vous à votre instance Windows.

2. Ouvrez le [site web NVIDIA](#) et sélectionnez la version de CUDA dont vous avez besoin.
3. Pour Installer Type (Type de programme d'installation, sélectionnez exe (local) puis choisissez Download (Télécharger).
4. À l'aide de votre navigateur, exécutez le fichier d'installation téléchargé. Suivez les instructions pour installer la boîte à outils CUDA. Vous devrez peut-être redémarrer l'instance.

Installez les pilotes AMD sur votre instance Amazon EC2

Une instance avec un GPU AMD attaché, telle qu'une instance G4ad, doit disposer du pilote AMD approprié installé. Selon vos exigences, vous pouvez utiliser une AMI avec un pilote préinstallé ou télécharger un pilote depuis Amazon S3.

Pour installer des pilotes NVIDIA sur une instance avec un GPU NVIDIA attaché, telle qu'une instance G4dn, reportez-vous à la section [Installer les pilotes NVIDIA](#).

Table des matières

- [Pilote AMD Radeon Pro Software for Enterprise](#)
- [AMI avec pilote AMD installé](#)
- [Téléchargement du pilote AMD](#)
- [Configuration d'un bureau interactif pour Linux](#)

Pilote AMD Radeon Pro Software for Enterprise

Le pilote AMD Radeon Pro Software for Enterprise est conçu pour fournir une prise en charge des cas d'utilisation graphiques de qualité professionnelle. À l'aide du pilote, vous pouvez configurer vos instances avec deux écrans 4K par GPU.

API prises en charge

- OpenGL, OpenCL
- Vulkan
- AMD Advanced Media Framework
- Video Acceleration API
- DirectX 9 et versions ultérieures
- Microsoft Hardware Media Foundation Transform

AMI avec pilote AMD installé

AWS propose différentes Amazon Machine Images (AMI) fournies avec les pilotes AMD installés. Ouvrez [les offres Marketplace avec le pilote AMD](#).

Téléchargement du pilote AMD

Si vous n'utilisez pas d'AMI avec le pilote AMD installé, vous pouvez télécharger le pilote AMD et l'installer sur votre instance. Seules les versions de système d'exploitation suivantes prennent en charge les pilotes AMD :

- Amazon Linux 2 avec la version 4.14 du noyau

Note

Les versions amdgpu-pro-20.20-1184451 et ultérieures du pilote AMD nécessitent la version 5.15 ou une version ultérieure du noyau.

- Windows Server 2016
- Windows Server 2019

Ces téléchargements ne sont disponibles que pour AWS les clients. Si vous téléchargez le pilote, vous acceptez d'employer le logiciel téléchargé uniquement pour développer des AMIs à utiliser avec le matériel AMD Radeon Pro V520. Dès l'installation du logiciel, vous êtes lié par les conditions du [Contrat de licence utilisateur final AMD Software](#).

Installez le pilote AMD sur votre instance Linux

1. Connectez-vous à votre instance Linux.
2. Installez-le AWS CLI sur votre instance Linux et configurez les informations d'identification par défaut. Pour plus d'informations, consultez [Installation d' AWS CLI](#) dans le Guide de l'utilisateur AWS Command Line Interface .

Important

Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'ReadOnlyaccès d'AmazonS3. Pour plus d'informations, consultez la [politique](#)

[AWS gérée : AmazonS3 ReadOnly Access](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

3. Installez gcc et make, si ce n'est pas déjà fait.

```
$ sudo yum install gcc make
```

4. Mettez à jour le cache de votre package et obtenez les mises à jour de packages pour votre instance.

- Dans Amazon Linux 2:

```
$ sudo amazon-linux-extras install epel -y  
$ sudo yum update -y
```

- Pour Ubuntu 22.04 :

```
$ wget https://repo.radeon.com/.preview/a0e4ef1dffbc95b4abb54e891f265e61/amdgpu-  
install/5.5.02.05.2/ubuntu/jammy/amdgpu-install_5.5.02.05.50502-1_all.deb  
$ sudo apt install ./amdgpu-install_5.5.02.05.50502-1_all.deb  
$ sudo sed -i 's#repo.radeon.com#&/.preview/a0e4ef1dffbc95b4abb54e891f265e61#' /  
etc/apt/sources.list.d/{amdgpu.list,rocm.list,amdgpu-proprietary.list}
```

- Pour les autres versions d'Ubuntu :

```
$ sudo dpkg --add-architecture i386  
$ sudo apt-get update -y && sudo apt upgrade -y
```

- Pour CentOS :

```
$ sudo yum install epel-release -y  
$ sudo yum update -y
```

5. Redémarrez l'instance.

```
$ sudo reboot
```

6. Reconnectez-vous à l'instance après son redémarrage.
7. Téléchargez le dernier pilote AMD.

Note

Ignorez cette étape pour Ubuntu 22.04.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

8. Extrayez le fichier.

- Pour Amazon Linux 2 et CentOS :

```
$ tar -xf amdgpu-pro-*rhel*.tar.xz
```

- Pour Ubuntu :

Note

Ignorez cette étape pour Ubuntu 22.04.

```
$ tar -xf amdgpu-pro*ubuntu*.xz
```

9. Sélectionnez le dossier du pilote extrait.

10. Ajoutez les modules manquants pour l'installation du pilote.

- Pour Amazon Linux 2 et CentOS :

Ignorez cette étape.

- Pour Ubuntu :

Note

Ignorez cette étape pour Ubuntu 22.04.

```
$ sudo apt install linux-modules-extra-$(uname -r) -y
```

11. Exécutez le script d'installation automatique pour installer la pile graphique complète.

- Pour Ubuntu 22.04 :

```
$ sudo amdgpu-install --usecase=workstation --vulkan=pro --opencl=rocr,legacy -y
```

- Pour Amazon Linux 2, CentOS et les autres versions d'Ubuntu :

```
$ ./amdgpu-pro-install -y --opencl=pa1,legacy
```

12. Redémarrez l'instance.

```
$ sudo reboot
```

13. Vérifiez que le pilote fonctionne.

```
$ dmesg | grep amdgpu
```

Les résultats doivent avoir l'aspect suivant :

```
Initialized amdgpu
```

Installez le pilote AMD sur votre instance Windows

1. Connectez-vous à votre instance Windows et ouvrez une PowerShell fenêtre.
2. Configurez les informations d'identification par défaut pour votre instance Windows. AWS Tools for Windows PowerShell Pour plus d'informations, voir [Démarrer avec les AWS Tools for Windows PowerShell](#) dans le Guide de l'utilisateur AWS Tools for Windows PowerShell .

Important

Votre utilisateur ou rôle doit disposer des autorisations accordées conformément à la politique d'ReadOnlyaccès d'AmazonS3. Pour plus d'informations, consultez la [politique AWS gérée : AmazonS3 ReadOnly Access](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

3. Téléchargez les pilotes depuis Amazon S3 sur votre bureau à l'aide des PowerShell commandes suivantes.

```

$Bucket = "ec2-amd-windows-drivers"
$KeyPrefix = "latest" # use "archives" for Windows Server 2016
$LocalPath = "$home\Desktop\AMD"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}

```

4. Décompressez le fichier de pilote téléchargé et exécutez le programme d'installation à l'aide des PowerShell commandes suivantes.

```

Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose

```

Vérifiez maintenant le contenu du nouveau répertoire. Le nom du répertoire peut être récupéré à l'aide de la `Get-ChildItem` PowerShell commande.

```

Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"

```

La sortie doit ressembler à ce qui suit :

```

Directory: C:\Users\Administrator\Desktop\AMD\latest

Mode                LastWriteTime         Length Name
----                -
d-----          10/13/2021  12:52 AM             210414a-365562C-Retail_End_User.2

```

Installez les pilotes :

```

pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs

```

5. Suivez les instructions pour installer le pilote et redémarrez votre instance le cas échéant.

6. Pour vous assurer que le GPU fonctionne correctement, vérifiez le Gestionnaire de périphériques. Vous devriez voir « AMD Radeon Pro V520 MxGPU » répertorié comme adaptateur graphique.
7. Pour profiter des quatre écrans d'une résolution allant jusqu'à 4K, configurez le protocole d'affichage haute performance, [NICE DCV](#).

Configuration d'un bureau interactif pour Linux

Après avoir vérifié que le pilote GPU AMD est installé sur votre instance Linux et qu'amdgpu est utilisé, vous pouvez installer un gestionnaire de bureau interactif. Nous recommandons l'environnement de travail MATE pour une compatibilité et des performances optimales.

Prérequis

Lancez un éditeur de texte et enregistrez ce qui suit en tant que fichier nommé `xorg.conf`. Vous aurez besoin de ce fichier sur votre instance.

```
Section "ServerLayout"
Identifier      "Layout0"
Screen         0 "Screen0"
InputDevice    "Keyboard0" "CoreKeyboard"
InputDevice    "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath    "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath    "/opt/amdgpu/lib/xorg/modules"
ModulePath    "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath    "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath    "/usr/lib64/xorg/modules"
ModulePath    "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier    "Mouse0"
Driver       "mouse"
Option       "Protocol" "auto"
Option       "Device" "/dev/psaux"
Option       "Emulate3Buttons" "no"
Option       "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
```

```
# generated from default
Identifier      "Keyboard0"
Driver          "kbd"
EndSection
Section "Monitor"
Identifier      "Monitor0"
VendorName      "Unknown"
ModelName       "Unknown"
EndSection
Section "Device"
Identifier      "Device0"
Driver          "amdgpu"
VendorName      "AMD"
BoardName       "Radeon MxGPU V520"
BusID           "PCI:0:30:0"
EndSection
Section "Extensions"
Option          "DPMS" "Disable"
EndSection
Section "Screen"
Identifier      "Screen0"
Device          "Device0"
Monitor         "Monitor0"
DefaultDepth    24
Option          "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual      3840 2160
    Depth        32
EndSubSection
EndSection
```

Pour configurer un bureau interactif sur Amazon Linux 2

1. Installez le référentiel EPEL.

```
$ C:\> sudo amazon-linux-extras install epel -y
```

2. Installez l'environnement de bureau MATE.

```
$ C:\> sudo amazon-linux-extras install mate-desktop1.x -y
$ C:\> sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copiez le fichier `xorg.conf` dans `/etc/X11/xorg.conf`.
4. Redémarrez l'instance.

```
$ C:\> sudo reboot
```

5. (Facultatif) [Installez le serveur NICE DCV](#) pour utiliser NICE DCV comme protocole d'affichage hautes performances, puis [connectez-vous à une session NICE DCV](#) à l'aide de votre client préféré.

Pour configurer un bureau interactif sur Ubuntu

1. Installez l'environnement de bureau MATE.

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y  
$ C:\> sudo apt purge ifupdown -y
```

2. Copiez le fichier `xorg.conf` dans `/etc/X11/xorg.conf`.
3. Redémarrez l'instance.

```
$ sudo reboot
```

4. Installez l'encodeur AMF pour la version appropriée d'Ubuntu.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Facultatif) [Installez le serveur NICE DCV](#) pour utiliser NICE DCV comme protocole d'affichage hautes performances, puis [connectez-vous à une session NICE DCV](#) à l'aide de votre client préféré.
6. Après l'installation de DCV, accordez les autorisations vidéo aux utilisateurs de DCV :

```
$ sudo usermod -aG video dcv
```

Pour configurer un bureau interactif sur CentOS

1. Installez le référentiel EPEL.

```
$ sudo yum update -y  
$ C:\> sudo yum install epel-release -y
```

2. Installez l'environnement de bureau MATE.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Copiez le fichier `xorg.conf` dans `/etc/X11/xorg.conf`.

4. Redémarrez l'instance.

```
$ sudo reboot
```

5. (Facultatif) [Installez le serveur NICE DCV](#) pour utiliser NICE DCV comme protocole d'affichage hautes performances, puis [connectez-vous à une session NICE DCV](#) à l'aide de votre client préféré.

Pilotes de virtualisation paravirtuelle pour les instances Windows

Les AMI Windows contiennent un jeu de pilotes permettant d'accéder au matériel virtualisé. Ces pilotes sont utilisés par Amazon EC2 pour mapper le stockage d'instances et les volumes Amazon EBS à leurs périphériques. Le tableau suivant présente les principales différences entre les différents pilotes.

	RedHat PV	Virtualisation paravirtuelle Citrix	AWS PV
Type d'instance	Non pris en charge pour tous les types d'instance. Si vous spécifiez un type d'instance non pris en charge, l'instance est dégradée.	Pris en charge pour les types d'instance Xen.	Pris en charge pour les types d'instance Xen.
Volumes attachés	Prend en charge jusqu'à 16 volumes attachés.	Prend en charge plus de 16 volumes attachés.	Prend en charge plus de 16 volumes attachés.

	RedHat PV	Virtualisation paravirtuelle Citrix	AWS PV
Réseau	<p>Le pilote rencontre des problèmes connus au cours desquels la connexion réseau se réinitialise en cas de charges élevées (les transferts de fichiers FTP rapides, par exemple).</p>		<p>Le pilote configure automatiquement des trames jumbo sur la carte réseau lorsqu'il se trouve sur un type d'instance compatible. Lorsque l'instance se trouve dans un groupe de placement de cluster, cela améliore les performances réseau entre les instances du groupe de placement de cluster. Pour plus d'informations, consultez</p>

	RedHat PV	Virtualisation paravirtuelle Citrix	AWS PV
			Groupes de placement.

Le tableau suivant présente les pilotes PV que vous devez exécuter sur chaque version de Windows Server sur Amazon EC2.

Version Windows Server	Version de pilote PV
Windows Server 2022	AWS Dernière version de PV
Windows Server 2019	AWS Dernière version de PV
Windows Server 2016	AWS Dernière version de PV
Windows Server 2012 R2	AWS Dernière version de PV
Windows Server 2012	AWS Dernière version de PV
Windows Server 2008 R2	AWS Version PC 8.3.5
Windows Server 2008	PV Citrix 5.9
Windows Server 2003	PV Citrix 5.9

Table des matières

- [AWS Pilotes photovoltaïques](#)
- [Pilotes PV Citrix](#)
- [RedHat Pilotes photovoltaïques](#)
- [S'abonner aux notifications](#)
- [Mise à niveau des pilotes PV sur les instances Windows](#)
- [Résoudre les problèmes liés aux pilotes PV sur les instances Windows](#)

AWS Pilotes photovoltaïques

Les pilotes AWS PV sont stockés dans le %ProgramFiles%\Amazon\Xentools répertoire. Ce répertoire contient également des symboles publics et un outil de ligne de commande qui vous permet d'accéder aux entrées de XenStore. `xenstore_client.exe` Par exemple, la PowerShell commande suivante renvoie l'heure actuelle depuis l'hyperviseur :

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
  AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

Les composants du pilote AWS PV sont répertoriés dans le registre Windows sous `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. Ces composants de pilote sont les suivants : `xenbus`, `xeniface`, `xennet`, `xenvbd` et `xenvif`.

AWS Les pilotes PV ont également un service Windows nommé `LiteAgent`, qui s'exécute en mode utilisateur. Il gère des tâches telles que les événements d'arrêt et de redémarrage à partir d' AWS API sur des instances de génération Xen. Vous pouvez accéder aux services et les gérer en exécutant `Services.msc` dans la ligne de commande. Lors de l'exécution sur des instances de génération Nitro, les pilotes AWS PV ne sont pas utilisés et le `LiteAgent` service s'arrête automatiquement à partir de la version 8.2.4 du pilote. La mise à jour vers le dernier pilote AWS PV permet également de mettre à jour `LiteAgent` et d'améliorer la fiabilité de toutes les générations d'instances.

Installez les derniers pilotes AWS PV

Les AMI Windows Amazon contiennent un jeu de pilotes permettant d'accéder au matériel virtualisé. Ces pilotes sont utilisés par Amazon EC2 pour mapper le stockage d'instances et les volumes Amazon EBS à leurs périphériques. Nous vous recommandons d'installer les derniers pilotes pour améliorer la stabilité et les performances des instances Windows EC2.

Options d'installation

- Vous pouvez l'utiliser AWS Systems Manager pour mettre à jour automatiquement les pilotes PV. Pour plus d'informations, consultez [Procédure de mise à jour automatique des pilotes PV sur les instances Windows EC2 \(console\)](#) dans le Guide de l'utilisateur AWS Systems Manager .
- Vous pouvez [télécharger](#) le package de pilotes et exécuter le programme d'installation manuellement. Consultez le fichier `readme.txt` pour connaître la configuration système requise. Pour plus d'informations sur le téléchargement et l'installation des pilotes PV AWS , ou si vous

mettez à niveau un contrôleur de domaine, consultez [Mettre à niveau les instances Windows Server \(mise à niveau AWS PV\) manuellement](#).

AWS Historique du package de pilotes PV

Le tableau suivant indique les modifications apportées aux pilotes AWS PV pour chaque version du pilote.

Version du package	Détails	Date de publication
8.4.3	Correction de bogues dans le programme d'installation du package afin d'améliorer l'expérience de mise à niveau.	24 janvier 2023
8.4.2	Correctifs de stabilité pour répondre aux conditions de concurrence.	13 avril 2022
8.4.1	Package d'installation amélioré.	7 janvier 2022
8.4.0	<ul style="list-style-type: none"> • Correctifs de stabilité pour traiter de rares cas d'IO de disque bloqué. • Correctifs de stabilité pour traiter les rares cas de plantages pendant le détachement du volume EBS. • Ajout d'une fonctionnalité pour répartir la charge sur plusieurs cœurs pour les charges de travail qui exploitent plus de 20 000 IOPS et subissent une dégradation due à des goulots d'étranglement. Pour activer cette fonctionnalité, consultez Les charges de travail qui exploitent plus de 20 000 IOPS disque subissent une dégradation due aux goulots d'étranglement du processeur. • AWS L'installation de PV 8.4 sur Windows Server 2008 R2 échouera. AWS Les versions PV 8.3.5 et antérieures sont prises en charge sur Windows Server 2008 R2. 	2 mars 2021
8.3.5	Package d'installation amélioré.	7 janvier 2022

Version du package	Détails	Date de publication
8.3.4	Amélioration de la fiabilité de la connexion des périphériques réseau.	4 août 2020
8.3.3	<ul style="list-style-type: none"> Mise à jour du composant XenStore orienté vers -facing pour empêcher la vérification des bogues lors des chemins de gestion des erreurs. Mise à jour vers le composant de stockage pour éviter les plantages lorsqu'un SRB non valide est soumis. <p>Pour mettre à jour ce pilote sur les instances Windows Server 2008 R2, vous devez d'abord vérifier que les correctifs appropriés sont installés de manière à répondre à l'avis de sécurité Microsoft suivant : Microsoft Security Advisory 3033929.</p>	4 février 2020
8.3.2	Fiabilité améliorée des composants de mise en réseau.	30 juillet 2019
8.3.1	Améliorations des performances et robustesse du composant de stockage.	12 juin 2019
8.2.7	Efficacité renforcée pour la prise en charge de la migration vers les types d'instance de dernière génération.	20 mai 2019
8.2.6	Amélioration de l'efficacité du chemin de vidage en cas de plantage.	15 janvier 2019
8.2.5	Améliorations de sécurité supplémentaires. PowerShell le programme d'installation est désormais disponible sous forme de package.	12 décembre 2018
8.2.4	Améliorations de la fiabilité.	2 octobre 2018

Version du package	Détails	Date de publication
8.2.3	<p>Correctifs de bogues et améliorations de performances.</p> <p>Rapport de l'ID de volume EBS comme numéro de série de disque pour les volumes EBS. Ceci permet des scénarios de cluster tels que S2D.</p>	29 mai 2018
8.2.1	<p>Amélioration des performances réseau et stockage, et correctifs de robustesse.</p> <p>Pour vérifier que cette version a été installée, reportez-vous à la valeur de registre Windows suivant : HKLM\Software\Amazon\PVDriver\Version 8.2.1 .</p>	8 mars 2018
7.4.6	<p>Correctifs de stabilité pour rendre les pilotes AWS photovolt aïques plus résilients.</p>	26 avril 2017
7.4.3	<p>Ajout de la prise en charge de Windows Server 2016.</p> <p>Correctifs de stabilité pour toutes les versions du système d'exploitation Windows prises en charge.</p> <p>* La signature du pilote AWS PV version 7.4.3 expire le 29 mars 2019. Nous vous recommandons de mettre à jour le pilote AWS PV le plus récent.</p>	18 nov 2016
7.4.2	<p>Correctifs de stabilité pour la prise en charge du type d'instance X1.</p>	2 août 2016

Version du package	Détails	Date de publication
7.4.1	<ul style="list-style-type: none">• Amélioration des performances du pilote de stockage AWS photovoltaïque.• Correctifs de stabilité dans le pilote AWS PV Storage : correction d'un problème à cause duquel les instances rencontraient un crash du système avec le code de vérification des bogues 0x0000DEAD.• Corrections de stabilité dans le pilote AWS PV Network.• Ajout de la prise en charge de Windows Server 2008 R2.	12 juillet 2016
7.3.2	<ul style="list-style-type: none">• Amélioration de la journalisation et des diagnostics.• Correctif de stabilité dans le pilote de stockage AWS PV. Dans certains cas, les disques n'apparaissent pas sur Windows après les avoir réassociés à l'instance.• Ajout de la prise en charge de Windows Server 2012.	24 juin 2015
7.3.1	Mise à jour de TRIM : correctif lié aux requêtes TRIM. Ce correctif stabilise les instances et améliore les performances des instances en cas de gestion d'un grand nombre de requêtes TRIM.	
7.3.0	Support TRIM : le pilote AWS PV envoie désormais des requêtes TRIM à l'hyperviseur. Les disques éphémères traitent correctement les requêtes TRIM étant donné que le stockage sous-jacent prend en charge TRIM (SSD). Notez que le stockage basé sur EBS ne prend plus en charge TRIM depuis mars 2015.	

Version du package	Détails	Date de publication
7.2.5	<ul style="list-style-type: none">• Correction de stabilité dans les pilotes de stockage AWS photovoltaïque : dans certains cas, le pilote AWS photovoltaïque peut déréférencer une mémoire non valide et provoquer une défaillance du système.• Correctif de stabilité lors de la génération d'un crash dump : dans certains cas, le pilote AWS photovoltaïque peut se retrouver bloqué dans des conditions de course lorsqu'il rédige un crash dump. Avant cette version, le seul moyen de résoudre ce problème était de forcer l'arrêt, puis le redémarrage du pilote afin de supprimer le fichier de vidage de mémoire.	
7.2.4	<p>Persistence de l'ID de l'appareil : ce correctif de pilote masque l'ID d'appareil PCI de la plateforme et oblige le système à renvoyer toujours le même ID d'appareil, même si l'instance est déplacée. De façon plus générale, ce correctif concerne la façon dont l'hyperviseur affiche les appareils virtuels. Le correctif inclut également des modifications apportées au co-installateur pour les pilotes AWS PV afin que le système conserve les périphériques virtuels mappés.</p>	
7.2.2	<ul style="list-style-type: none">• Chargez les pilotes AWS PV en mode DSRM (Directory Services Restore Mode) : le mode de restauration des services d'annuaire est une option de démarrage en mode sécurisé pour les contrôleurs de domaine Windows Server.• Persistence de l'ID de l'appareil lorsque la carte réseau virtuelle est rattachée : ce correctif oblige le système à vérifier le mappage de l'adresse MAC et assure la persistance de l'ID de l'appareil. Il garantit que les cartes réseau rattachées conservent leurs paramètres statiques.	

Version du package	Détails	Date de publication
7.2.1	<ul style="list-style-type: none"> Exécution en mode sans échec : résolution du problème empêchant le chargement du pilote en mode sans échec. Auparavant, les pilotes AWS PV n'étaient instanciés que dans les systèmes fonctionnant normalement. Ajout de disques aux groupes de stockage Microsoft Windows : précédemment, nous synthétisons les requêtes de page 83. Ce correctif a désactivé la prise en charge de page 83. Notez que cela ne concerne pas les groupes de stockage qui sont utilisés dans un environnement de cluster, car les disques PV ne sont pas des disques de cluster valides. 	
7.2.0	Base : version de base AWS PV.	

Pilotes PV Citrix

Les pilotes PV Citrix sont stockés dans le répertoire %ProgramFiles%\Citrix\XenTools (instances 32 bits) ou %ProgramFiles(x86)%\Citrix\XenTools (instances 64 bits).

Les composants de pilote PV Citrix sont répertoriés dans le registre Windows sous HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services. Ces composants de pilote sont les suivants : xenevtchn, xeniface, xennet, XenNet6, xensvc, xenvbd et xenvif.

Citrix possède également un composant pilote nommé XenGuestAgent, qui s'exécute en tant que service Windows. Il gère des tâches comme l'arrêt et le redémarrage d'événements dans l'API. Vous pouvez accéder aux services et les gérer en exécutant Services.msc dans la ligne de commande.

Si vous rencontrez des erreurs de mise en réseau lors de l'exécution de certaines charges de travail, vous pouvez devoir désactiver la fonction de transfert de la charge TCP pour le pilote PV Citrix. Pour plus d'informations, consultez [Transfert de la charge TCP](#).

RedHat Pilotes photovoltaïques

RedHat les pilotes sont pris en charge pour les anciennes instances, mais ne sont pas recommandés sur les nouvelles instances dotées de plus de 12 Go de RAM en raison des limitations des pilotes. Les instances dotées de plus de 12 Go de RAM exécutant des RedHat pilotes peuvent ne pas

démarrer et devenir inaccessibles. Nous recommandons de mettre à niveau RedHat les pilotes vers des pilotes PV Citrix, puis de mettre à niveau les pilotes PV Citrix vers des pilotes AWS PV.

Les fichiers source des RedHat pilotes se trouvent dans le répertoire %ProgramFiles%\RedHat (instances 32 bits) ou %ProgramFiles(x86)%\RedHat (instances 64 bits). Les deux pilotes sont `rhe1net` le pilote réseau RedHat paravirtualisé et `rhe1scsi` le pilote de miniport RedHat SCSI.

S'abonner aux notifications

Amazon SNS peut vous notifier en cas de publication de nouvelles versions des pilotes Windows EC2. Utilisez l'une des méthodes suivantes pour vous abonner à ces notifications.

Note

Vous devez spécifier la région de la rubrique SNS à laquelle vous êtes abonné.

S'abonner aux notifications EC2 à partir de la console

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région, car les notifications SNS auxquelles vous vous abonnez sont dans cette région.
3. Dans le panneau de navigation, choisissez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :
 - a. Pour TopicARN, copiez l'Amazon Resource Name (ARN) suivant :
`arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers`
 - b. Pour Protocole, choisissez Email.
 - c. Pour Point de terminaison, tapez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications.
 - d. Choisissez Créer un abonnement.
6. Vous recevrez rapidement un e-mail de confirmation. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Abonnez-vous aux notifications EC2 à l'aide du AWS CLI

Pour vous abonner aux notifications EC2 avec le AWS CLI, utilisez la commande suivante.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-  
windows-drivers --region us-east-1 --protocol email --notification-  
endpoint YourUserName@YourDomainName.ext
```

Abonnez-vous aux notifications EC2 à l'aide du AWS Tools for PowerShell

Pour vous abonner aux notifications EC2 avec Tools for Windows PowerShell, utilisez la commande suivante.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-  
drivers' -Region us-east-1 -Protocol email -Endpoint 'YourUserName@YourDomainName.ext'
```

Chaque fois que des pilotes Windows EC2 sont publiés, nous envoyons des notifications aux abonnés de la rubrique . Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Se désinscrire des notifications des pilotes Windows Amazon EC2

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans le panneau de navigation, choisissez Abonnements.
3. Cochez la case correspondant à l'abonnement, puis choisissez Actions, Supprimer des abonnements. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Mise à niveau des pilotes PV sur les instances Windows

Nous vous recommandons d'installer les derniers pilotes PV pour améliorer la stabilité et les performances des instances Windows EC2. Les instructions sur cette page vous aident à télécharger le package de pilotes et à exécuter le programme d'installation.

Pour vérifier quel pilote votre instance Windows utilise

Ouvrez Connexions réseau dans le Panneau de configuration et affichez Connexion au réseau local. Vérifiez si le pilote est l'un des suivants :

- AWS Dispositif de réseau PV
- Carte Ethernet PV Citrix
- RedHat Pilote PV NIC

Sinon, vous pouvez vérifier la sortie de la commande `pnputil -e`.

Configuration système requise

Consultez le fichier `readme.txt` pour connaître la configuration système requise.

Table des matières

- [Mettre à niveau les instances Windows Server \(mise à niveau AWS PV\) avec Distributor](#)
- [Mettre à niveau les instances Windows Server \(mise à niveau AWS PV\) manuellement](#)
- [Mettre à niveau un contrôleur de domaine \(mise à niveau AWS PV\)](#)
- [Mise à niveau des instances Windows Server 2008 et 2008 R2 \(Mise à niveau d'un PV Redhat vers Citrix\)](#)
- [Mettre à niveau votre service d'agent invité Citrix Xen](#)

Mettre à niveau les instances Windows Server (mise à niveau AWS PV) avec Distributor

Vous pouvez utiliser Distributor, une fonctionnalité de AWS Systems Manager, pour installer ou mettre à niveau le package de pilotes AWS PV. L'installation ou la mise à niveau peut être effectuée une seule fois, ou vous pouvez l'installer ou la mettre à jour selon un calendrier. L'In-place update option Type d'installation n'est pas prise en charge pour ce package de distribution.

Important

Si votre instance est un contrôleur de domaine, consultez [Mettre à niveau un contrôleur de domaine \(mise à niveau AWS PV\)](#). Le processus de mise à niveau pour les instances de contrôleur de domaine est différent de celui des éditions standard de Windows.

1. Nous vous recommandons de créer une sauvegarde au cas où vous auriez besoin d'annuler vos modifications.

 Tip

Au lieu de créer l'AMI depuis la console Amazon EC2, vous pouvez utiliser Systems Manager Automation pour créer l'AMI à l'aide du `AWS-CreateImage` runbook. Pour plus d'informations, consultez le Guide [AWS-CreateImage](#) de l'utilisateur de référence du runbook AWS Systems Manager Automation.

- a. Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Avant d'arrêter une instance, vérifiez que vous avez copié toutes les données dont vous avez besoin à partir de vos volumes de stockage d'instances vers un stockage persistant, tel que Amazon EBS ou Amazon S3.
 - b. Dans le panneau de navigation, choisissez Instances.
 - c. Sélectionnez l'instance qui nécessite la mise à niveau du pilote, puis État de l'instance, Arrêter l'instance.
 - d. Une fois l'instance arrêtée, sélectionnez l'instance, puis Actions, Image et modèles, et enfin Créer une image.
 - e. Choisissez État de l'instance, Démarrer l'instance.
2. Se connecter à l'instance en utilisant le Bureau à distance. Pour plus d'informations, consultez [the section called "Connectez-vous à votre instance Windows à l'aide d'un client RDP"](#).
 3. Nous vous recommandons d'utiliser des disques non système hors ligne et de prendre en compte les drive mappages de lettres de lecteurs aux disques secondaires dans Gestion des disques avant d'exécuter cette mise à niveau. Cette étape n'est pas obligatoire si vous effectuez une mise à jour sur place des pilotes AWS PV. Nous vous recommandons également de définir les services non essentiels sur le start-up Manuel dans la console Services.
 4. Pour les instructions relatives à l'installation ou à la mise à niveau du package de pilotes AWS PV à l'aide de Distributor, reportez-vous aux procédures décrites dans la section [Installer ou mettre à jour des packages](#) dans le guide de AWS Systems Manager l'utilisateur.
 5. Dans Nom, choisissez AWSPVDriver.
 6. Pour le type d'installation, sélectionnez Désinstaller et réinstallez.
 7. Configurez les autres paramètres du package selon les besoins et exécutez l'installation ou la mise à niveau à l'aide de la procédure référencée dans [Step 4](#).

Après avoir exécuté le package Distributor, l'instance redémarre automatiquement puis met à niveau le pilote. L'instance ne sera pas disponible pendant 15 minutes.

8. Une fois la mise à niveau terminée et l'instance passée avec succès les deux tests de santé dans la console Amazon EC2, vérifiez que le nouveau pilote a été installé en vous connectant à l'instance via Remote Desktop.
9. Une fois connecté, exécutez la PowerShell commande suivante :

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

10. Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez [AWS Historique du package de pilotes PV](#) Open Disk Management pour passer en revue les volumes secondaires hors ligne et les mettre en ligne conformément aux lettres de lecteur indiquées dans [Step 3](#).

Si vous avez précédemment désactivé [Transfert de la charge TCP](#) l'utilisation de Netsh pour les pilotes PV Citrix, nous vous recommandons de réactiver cette fonctionnalité après la mise à niveau vers les pilotes AWS PV. Les problèmes de déchargement TCP liés aux pilotes Citrix ne sont pas présents dans les pilotes AWS PV. Par conséquent, le déchargement TCP offre de meilleures performances avec les pilotes AWS PV.

Si vous avez déjà appliqué une adresse IP statique ou une configuration DNS à l'interface réseau, vous devrez peut-être réappliquer l'adresse IP statique ou la configuration DNS après la mise à niveau des pilotes AWS PV.

Mettre à niveau les instances Windows Server (mise à niveau AWS PV) manuellement

Utilisez la procédure suivante pour effectuer une mise à niveau sur place des pilotes AWS PV ou pour passer des pilotes PV Citrix aux pilotes AWS PV sous Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 ou Windows Server 2022. Cette mise à niveau n'est pas disponible pour RedHat les pilotes, ni pour les autres versions de Windows Server.

Certaines anciennes versions de Windows Server ne peuvent pas utiliser les derniers pilotes. Pour vérifier la version du pilote à utiliser pour votre système d'exploitation, consultez le tableau des versions de pilotes de la page [Pilotes de virtualisation paravirtuelle pour les instances Windows](#).

⚠ Important

Si votre instance est un contrôleur de domaine, consultez [Mettre à niveau un contrôleur de domaine \(mise à niveau AWS PV\)](#). Le processus de mise à niveau pour les instances de contrôleur de domaine est différent de celui des éditions standard de Windows.

Pour mettre à niveau les pilotes AWS PV manuellement

1. Nous vous recommandons de créer une sauvegarde au cas où vous auriez besoin d'annuler vos modifications.

ℹ Tip

Au lieu de créer l'AMI depuis la console Amazon EC2, vous pouvez utiliser Systems Manager Automation pour créer l'AMI à l'aide du [AWS-CreateImage](#) runbook. Pour plus d'informations, consultez le Guide [AWS-CreateImage](#) de l'utilisateur de référence du runbook AWS Systems Manager Automation.

- a. Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Avant d'arrêter une instance, vérifiez que vous avez copié toutes les données dont vous avez besoin à partir de vos volumes de stockage d'instances vers un stockage persistant, tel que Amazon EBS ou Amazon S3.
 - b. Dans le panneau de navigation, choisissez Instances.
 - c. Sélectionnez l'instance qui nécessite la mise à niveau du pilote, puis État de l'instance, Arrêter l'instance.
 - d. Une fois l'instance arrêtée, sélectionnez l'instance, puis Actions, Image et modèles, et enfin Créer une image.
 - e. Choisissez État de l'instance, Démarrer l'instance.
2. Se connecter à l'instance en utilisant le Bureau à distance.
 3. Nous vous recommandons d'utiliser des disques non système hors ligne et de prendre en compte les drive mappages de lettres de lecteurs aux disques secondaires dans Gestion des disques avant d'exécuter cette mise à niveau. Cette étape n'est pas obligatoire si vous effectuez une mise à jour sur place des pilotes AWS PV. Nous vous recommandons également de définir les services non essentiels sur le start-up Manuel dans la console Services.

4. [Téléchargez](#) le package de pilotes le plus récent sur l'instance.

Vous pouvez également exécuter la PowerShell commande suivante :

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/
Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath
$env:userprofile\pv_drivers
```

Note

Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que le protocole TLS 1.2 doive être activé sur votre PowerShell terminal. Vous pouvez activer le protocole TLS 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
```

5. Extrayez le contenu du dossier, puis exécutez `AWSPVDriverSetup.msi`.

Après avoir exécuté le MSI, l'instance redémarre automatiquement puis met à niveau le pilote. L'instance ne sera pas disponible pendant 15 minutes. Une fois la mise à niveau terminée et l'instance passée avec succès les deux tests de santé dans la console Amazon EC2, vous pouvez vérifier que le nouveau pilote a été installé en vous connectant à l'instance via Remote Desktop, puis en exécutant la commande suivante : PowerShell

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez [AWS Historique du package de pilotes PV](#) Open Disk Management pour passer en revue les volumes secondaires hors ligne et les mettre en ligne conformément aux lettres de lecteur indiquées dans [Step 3](#).

Si vous avez précédemment désactivé [Transfert de la charge TCP](#) l'utilisation de Netsh pour les pilotes PV Citrix, nous vous recommandons de réactiver cette fonctionnalité après la mise à niveau vers les pilotes AWS PV. Les problèmes de déchargement TCP liés aux pilotes Citrix ne sont pas

présents dans les pilotes AWS PV. Par conséquent, le déchargement TCP offre de meilleures performances avec les pilotes AWS PV.

Si vous avez déjà appliqué une adresse IP statique ou une configuration DNS à l'interface réseau, vous devrez peut-être réappliquer l'adresse IP statique ou la configuration DNS après la mise à niveau des pilotes AWS PV.

Mettre à niveau un contrôleur de domaine (mise à niveau AWS PV)

Utilisez la procédure suivante sur un contrôleur de domaine pour effectuer une mise à niveau sur place des pilotes AWS PV ou pour passer des pilotes PV Citrix aux pilotes AWS PV.

Pour mettre à niveau un contrôleur de domaine

1. Nous vous recommandons de créer une sauvegarde de votre contrôleur de domaine au cas où vous auriez besoin d'annuler vos modifications. L'utilisation d'une AMI en tant que sauvegarde n'est pas prise en charge. Pour plus d'informations, consultez [Considérations de sauvegarde et de restauration pour les contrôleurs de domaine virtualisés](#) dans la documentation Microsoft.
2. Exécutez la commande suivante afin de configurer Windows pour démarrer en mode DSRM (Directory Services Restore Mode).

 Warning

Avant d'exécuter cette commande, vérifiez que vous connaissez le mot de passe DSRM. Vous aurez besoin de ces informations pour vous connecter à votre instance une fois que la mise à niveau est terminée et que l'instance redémarre automatiquement.

```
bcdedit /set {default} safeboot dsrepair
```

PowerShell:

```
PS C:\> bcdedit /set "{default}" safeboot dsrepair
```

Le système doit démarrer en DSRM car l'utilitaire de mise à niveau supprime les pilotes de stockage PV Citrix afin de pouvoir installer les pilotes AWS PV. Nous vous recommandons donc de noter les lettres de lecteur et mappages de dossiers aux disques secondaires dans Gestion des disques. En l'absence de pilote de stockage PV Citrix, les disques secondaires ne sont pas

détectés. Les contrôleurs de domaine qui utilisent un dossier NTDS sur des disques secondaires ne démarreront pas, car le disque secondaire ne sera pas détecté.

⚠ Warning

Après avoir exécuté cette commande, ne redémarrez pas le système manuellement. Le système sera inaccessible du fait que les pilotes PV Citrix ne prennent pas en charge le DSRM.

3. Exécutez la commande suivante pour ajouter **DisableDCCheck** au registre :

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t REG_SZ /d true
```

4. [Téléchargez](#) le package de pilotes le plus récent sur l'instance.
5. Extrayez le contenu du dossier, puis exécutez `AWSPVDriverSetup.msi`.

Après avoir exécuté le MSI, l'instance redémarre automatiquement puis met à niveau le pilote. L'instance ne sera pas disponible pendant 15 minutes.

6. Une fois la mise à niveau terminée et que l'instance réussit les deux vérifications de l'état dans la console Amazon EC2, connectez-vous à l'instance à l'aide des services Bureau à distance. Ouvrez Gestion des disques pour vérifier la présence de volumes secondaires hors ligne et les mettre en ligne en les faisant correspondre aux lettres des lecteurs et aux mappages de dossiers notés précédemment.

Vous devez vous connecter à l'instance en spécifiant le nom utilisateur selon le format `nom_hôte\administrator`. Par exemple, `Win2k12 \ administratorTestBox`.

7. Exécutez la commande suivante pour supprimer la configuration du démarrage DSRM :

```
bcdedit /deletevalue safeboot
```

8. Redémarrez l'instance.
9. Pour exécuter le processus de mise à niveau, vérifiez que le nouveau pilote a été installé. Dans le Gestionnaire de périphériques, sous Contrôleurs de stockage, recherchez Carte hôte AWS PV Storage. Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez [AWS Historique du package de pilotes PV](#).
10. Exécutez la commande suivante pour supprimer **DisableDCCheck** du registre :

```
reg delete HKLM\SOFTWARE Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
```

Note

Si vous avez précédemment désactivé [Transfert de la charge TCP](#) l'utilisation de Netsh pour les pilotes PV Citrix, nous vous recommandons de réactiver cette fonctionnalité après la mise à niveau vers les pilotes AWS PV. Les problèmes de déchargement TCP liés aux pilotes Citrix ne sont pas présents dans les pilotes AWS PV. Par conséquent, le déchargement TCP offre de meilleures performances avec les pilotes AWS PV.

Mise à niveau des instances Windows Server 2008 et 2008 R2 (Mise à niveau d'un PV Redhat vers Citrix)

Avant de commencer à mettre à niveau vos RedHat pilotes vers les pilotes PV Citrix, assurez-vous de suivre les étapes suivantes :

- Installation de la version la plus récente du service EC2Config. Pour plus d'informations, consultez [Installer la dernière version d'EC2Config](#).
- Vérifiez que Windows PowerShell 3.0 est installé. Pour vérifier la version que vous avez installée, exécutez la commande suivante dans une PowerShell fenêtre :

```
PS C:\> $PSVersionTable.PSVersion
```

Windows PowerShell 3.0 est inclus dans le package d'installation de Windows Management Framework (WMF) version 3.0. Si vous devez installer Windows PowerShell 3.0, consultez la section [Windows Management Framework 3.0](#) dans le Microsoft Download Center.

- Sauvegardez vos informations importantes sur l'instance ou créez une AMI à partir de l'instance. Pour plus d'informations sur la création d'une AMI, consultez [Création d'une AMI basée sur Amazon EBS](#).

Tip

Au lieu de créer l'AMI depuis la console Amazon EC2, vous pouvez utiliser Systems Manager Automation pour créer l'AMI à l'aide du AWS-CreateImage runbook. Pour

plus d'informations, consultez le Guide [AWS-CreatImage](#) de l'utilisateur de référence du runbook AWS Systems Manager Automation.

Avant de créer une AMI, veuillez à exécuter les actions suivantes :

- Prenez note de votre mot de passe.
- N'exécutez pas l'outil Sysprep manuellement ou à l'aide du service EC2Config.
- Définissez votre carte Ethernet pour obtenir une adresse IP automatiquement à l'aide de DHCP. Pour plus d'informations, voir [Configurer les paramètres TCP/IP dans](#) la Microsoft Library. TechNet

Pour mettre à niveau RedHat les pilotes

1. Connectez-vous à votre instance en tant qu'administrateur local. Pour plus d'informations sur la connexion à votre instance, consultez [Connexion à votre instance Windows](#).
2. Dans votre instance, [téléchargez](#) le package de mise à niveau de PV Citrix.
3. Extrayez le contenu du package de mise à niveau à un emplacement de votre choix.
4. Double-cliquez sur le fichier Upgrade.bat. Si vous recevez un avertissement de sécurité, cliquez sur Run (Exécuter).
5. Dans la boîte de dialogue Upgrade Drivers (Mettre à niveau les pilotes), consultez les informations et cliquez sur Yes (Oui) si vous êtes prêt à démarrer la mise à niveau.
6. Dans la boîte de dialogue de désinstallation des pilotes Xen paravirtualisés Red Hat pour Windows, choisissez Oui pour supprimer le logiciel. RedHat Votre instance va être redémarrée.

Note

Si la boîte de dialogue du programme de désinstallation ne s'affiche pas, cliquez sur Red Hat Paravirtualize... dans la barre des tâches de Windows.



7. Vérifiez que l'instance a été redémarrée et qu'elle est prête à être utilisée.
 - a. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

- b. Sur la page Instances, sélectionnez Actions, Surveiller et dépanner, puis Obtenir le journal système.
- c. Les opérations de mise à niveau doivent avoir redémarré le serveur 3 ou 4 fois. Vous pouvez vous en assurer dans le fichier journal avec le nombre de fois où Windows is Ready to use s'affiche.

```

Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
Ec2Config service v2.1.9.0
RedHat PV NIC Driver v1.3.10.0
2013/03/15 17:11:01Z: Waiting for meta-data accessibility...
2013/03/15 17:11:02Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
<Username>Administrator</Username>
<Password>
L79ThJPF8LyIL38I2ht0FBrjet3vnT2csTiU/XGVMRCH7kQtBznAnXrKd1sirXlx19BwVMsd9b38jFJqv01IUpgNNJRZoCdc7IbUw
</Password>
2013/03/15 17:11:30Z: Product activation was successful.
2013/03/15 17:11:32Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
Ec2Config service v2.1.9.0
2013/03/15 21:04:24Z: There was an exception writing driver information to console: System.Exception: U
at Ec2Config.Service1.Go()
2013/03/15 21:04:35Z: Waiting for meta-data accessibility...
2013/03/15 21:04:40Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:05:08Z: Product activation was successful.
2013/03/15 21:05:09Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
Ec2Config service v2.1.9.0
Citrix PV Ethernet Adapter v5.9.960.49119
2013/03/15 21:07:20Z: Waiting for meta-data accessibility...
2013/03/15 21:07:21Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:07:27Z: Message: Windows is Ready to use

```

8. Connectez-vous à votre instance en tant qu'administrateur local.
9. Fermez la boîte de dialogue Red Hat Paravirtualized Xen Drivers for Windows uninstaller (Programme de désinstallation des pilotes Xen Red Hat Paravirtualize pour Windows).
10. Confirmez que l'installation est terminée. Accédez au dossier Citrix-WIN_PV que vous avez extrait précédemment, ouvrez le fichier PVUpgrade.log, puis recherchez le texte INSTALLATION IS COMPLETE.

```

PVUpgrade - Notepad
File Edit Format View Help
20130315_0905:25 #reinstall Device PCI\IDE\IDECHANNEL\4480001ED6060
20130315_0905:33 #reinstall Device PCI\VEN_8086&DEV_7010&SUBSYS_00015853&REV_00\3&267A616A&0609
20130315_0905:43 #reinstall Device ACPI\PNP0A03\0
20130315_0905:49 #removing Service: rhei\filter
20130315_0905:49 #removing Service: rhei-net
20130315_0905:49 #removing Driver File: C:\windows\System32\drivers\rheiflter.sys
20130315_0905:50 #removing Driver File: C:\windows\System32\drivers\rhei-net.sys
20130315_0905:50 #removing Redhat Service: C:\windows\System32\rheisvc.exe
20130315_0905:50 Unable to delete File, need to restart
20130315_0905:50 -----
20130315_0905:50 Restarting computer...
20130315_0905:50 -----
20130315_0907:05 START: 20130315_0907
20130315_0907:05 Running as: SYSTEM
20130315_0907:05 Current Running Directory: C:\Users\Administrator\downloads\Citrix-win_PV
20130315_0907:05 Detecting windows version
20130315_0907:16 #reinstall Device PCI\IDE\IDECHANNEL\4480001ED6060
20130315_0907:42 #reinstall Device PCI\IDE\IDECHANNEL\4480001ED6060
20130315_0907:49 #reinstall Device PCI\VEN_8086&DEV_7010&SUBSYS_00015853&REV_00\3&267A616A&0609
20130315_0907:57 #reinstall Device ACPI\PNP0A03\0
20130315_0908:05 #removing Redhat Service: C:\windows\System32\rheisvc.exe
20130315_0908:05 #removing Driver File: C:\windows\System32\drivers\rheiscsi.sys
20130315_0908:08 Adding First Surprise Removal Item
20130315_0908:08 Adding last surprise Removal Item
20130315_0908:08 Edits Saved
20130315_0908:08 Setting Existing Disks for Quick Removal
20130315_0908:08 Adding Quick Removal Settings to: C:\windows\System32\DriverStore\FileRepository\disk.inf_126712d3\disk.inf
20130315_0908:08 Adding First Surprise Removal Item
20130315_0908:08 Adding last Surprise Removal Item
20130315_0908:08 Edits Saved
20130315_0908:08 Setting Existing Disks for Quick Removal
20130315_0908:08 complete
20130315_0908:08 Removing Scheduled Task
20130315_0908:09
20130315_0908:09 IMPORTANT: Please uninstall any remaining Redhat Driver software from Add/Remove Programs
20130315_0908:09 INSTALLATION IS COMPLETE
20130315_0908:09 Setting Powershell script execution policy to Restricted
  
```

Mettre à niveau votre service d'agent invité Citrix Xen

Si vous utilisez des pilotes PV Citrix sur Windows Server, vous pouvez mettre à niveau le service d'agent invité Citrix Xen. Ce service Windows gère des tâches comme l'arrêt et le redémarrage d'événements dans l'API. Vous pouvez exécuter ce package de mise à niveau sur toute version de Windows Server dans la mesure où l'instance exécute des pilotes PV Citrix.

Important

Pour Windows Server 2008 R2 et versions ultérieures, nous vous recommandons de passer aux pilotes AWS PV qui incluent la mise à jour de l'agent invité.

Avant de commencer la mise à niveau de vos pilotes, veuillez à sauvegarder vos informations importantes sur l'instance ou créez une AMI à partir de l'instance. Pour plus d'informations sur la création d'une AMI, consultez [Création d'une AMI basée sur Amazon EBS](#).

Tip

Au lieu de créer l'AMI depuis la console Amazon EC2, vous pouvez utiliser Systems Manager Automation pour créer l'AMI à l'aide du AWS-CreateImage runbook. Pour plus

d'informations, consultez le Guide [AWS-CreatelImage](#) de l'utilisateur de référence du runbook AWS Systems Manager Automation.

Avant de créer une AMI, veuillez à exécuter les actions suivantes :

- N'activez pas l'outil Sysprep dans le service EC2Config.
- Prenez note de votre mot de passe.
- Définissez votre carte Ethernet sur DHCP.

Pour mettre à niveau votre service d'agent invité Citrix Xen

1. Connectez-vous à votre instance en tant qu'administrateur local. Pour plus d'informations sur la connexion à votre instance, consultez [Connexion à votre instance Windows](#).
2. Dans votre instance, [téléchargez](#) le package de mise à niveau de Citrix.
3. Extrayez le contenu du package de mise à niveau à un emplacement de votre choix.
4. Double-cliquez sur le fichier Upgrade.bat. Si vous recevez un avertissement de sécurité, cliquez sur Run (Exécuter).
5. Dans la boîte de dialogue Upgrade Drivers (Mettre à niveau les pilotes), consultez les informations et cliquez sur Yes (Oui) si vous êtes prêt à démarrer la mise à niveau.
6. Une fois la mise à niveau terminée, le fichier PVUpgrade.log s'ouvre et affiche le texte UPGRADE IS COMPLETE.
7. Redémarrez votre instance.

Résoudre les problèmes liés aux pilotes PV sur les instances Windows

Les informations suivantes constituent des solutions à des problèmes que vous pouvez rencontrer avec des images Amazon EC2 et pilotes PV plus anciens.

Sommaire

- [Windows Server 2012 R2 perd la connectivité au réseau ou à l'unité de stockage après le redémarrage d'une instance](#)
- [Transfert de la charge TCP](#)
- [Synchronisation du temps](#)

- [Les charges de travail qui exploitent plus de 20 000 IOPS disque subissent une dégradation due aux goulots d'étranglement du processeur](#)

Windows Server 2012 R2 perd la connectivité au réseau ou à l'unité de stockage après le redémarrage d'une instance

 Important

Ce problème se produit uniquement avec des AMI disponibles avant septembre 2014.

Les Amazon Machine Image (AMI) Windows Server 2012 R2 antérieures au 10 septembre 2014 peuvent perdre la connectivité au réseau et au stockage après un redémarrage de l'instance. L'erreur dans le journal du AWS Management Console système indique : « Difficulté à détecter les détails du pilote PV pour la sortie de console ». La perte de connectivité est causée par la fonction de nettoyage Plug and Play. Cette fonction recherche et désactive les périphériques système inactifs tous les 30 jours. Elle identifie à tort le périphérique réseau EC2 comme étant inactif et le supprime du système. Le cas échéant, l'instance perd la connectivité au réseau après un redémarrage.

Pour les systèmes que vous soupçonnez d'être vulnérables à ce problème, vous pouvez télécharger et exécuter une mise à niveau de pilote sur place. Si vous ne parvenez pas à effectuer la mise à jour du pilote sur place, vous pouvez exécuter un script d'assistant. Ce script détermine si le problème affecte votre instance. Si tel est le cas et que le périphérique réseau Amazon EC2 n'a pas encore été supprimé, le script désactive l'analyse de la fonctionnalité de nettoyage Plug and Play. Si le périphérique réseau a été supprimé, le script le répare, désactive l'analyse de la fonctionnalité de nettoyage Plug and Play et laisse l'instance redémarrer avec la connectivité réseau activée.

Sommaire

- [Choisir comment résoudre les problèmes](#)
- [Méthode 1 - Mise en réseau améliorée](#)
- [Méthode 2 - Configuration du registre](#)
- [Exécuter le script de correction](#)

Choisir comment résoudre les problèmes

Deux méthodes vous permettent de restaurer la connectivité au réseau et au stockage d'une instance affectée par ce problème. Choisissez l'une des méthodes suivantes :

Méthode	Prérequis	Présentation de la procédure
Méthode 1 - Mise en réseau améliorée	La mise en réseau améliorée est disponible uniquement dans un Virtual Private Cloud (VPC) nécessitant un type d'instance C3. Si le serveur n'utilise pas le type d'instance C3 actuellement, vous devez le modifier temporairement.	Vous modifiez le type d'instance du serveur pour une instance C3. La mise en réseau améliorée vous permet de vous connecter à l'instance affectée pour résoudre le problème. Une fois le problème résolu, vous modifiez à nouveau l'instance pour revenir au type d'instance original. Cette méthode est généralement plus rapide que la Méthode 2 et risque moins d'entraîner des erreurs d'utilisateur. Des frais supplémentaires seront facturés tant que l'instance C3 sera en cours d'exécution.
Méthode 2 - Configuration du registre	Capacité à créer ou à accéder à un second serveur. Capacité à modifier les paramètres du registre.	Démontez et détachez le volume racine à partir de l'instance affectée, attachez-le à une autre instance et effectuez les modifications dans le registre. Des frais supplémentaires seront facturés tant que le serveur supplémentaire sera en cours d'exécution. Cette méthode est plus lente que la Méthode 1, mais elle a fonctionné dans certaines situations dans lesquelles

Méthode	Prérequis	Présentation de la procédure
		la Méthode 1 a échoué à résoudre le problème.

Méthode 1 - Mise en réseau améliorée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Recherchez l'instance concernée. Sélectionnez l'instance, État de l'instance, puis Arrêter l'instance.

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Une fois l'instance arrêtée, créez une sauvegarde. Sélectionnez l'instance, puis Actions, Image et modèles, et enfin Créer une image.
5. [Modifiez](#) le type d'instance avec un n'importe quel type d'instance C3.
6. [Démarez](#) l'instance.
7. Connectez-vous à l'instance à l'aide de Remote Desktop, puis [téléchargez](#) le package AWS PV Drivers Upgrade sur l'instance.
8. Extrayez le contenu du dossier, puis exécutez `AWSPVDriverSetup.msi`.

Après avoir exécuté le MSI, l'instance redémarre automatiquement puis met à niveau les pilotes. L'instance ne sera pas disponible pendant 15 minutes.

9. Une fois la mise à niveau terminée et que l'instance réussit les deux vérifications de l'état dans la console Amazon EC2, connectez-vous à l'instance à l'aide des services Bureau à distance et vérifiez que les nouveaux pilotes ont été installés. Dans le Gestionnaire de périphériques, sous Contrôleurs de stockage, recherchez Carte hôte AWS PV Storage. Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez [AWS Historique du package de pilotes PV](#).
10. Arrêtez l'instance et modifiez-la à nouveau pour revenir à son type d'instance original.

11. Démarrez l'instance et reprenez une utilisation normale.

Méthode 2 - Configuration du registre

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Recherchez l'instance concernée. Sélectionnez l'instance, État de l'instance, puis Arrêter l'instance.

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Sélectionnez Lancer des instances et créez une instance Windows Server 2008 ou Windows Server 2012 dans la même zone de disponibilité que l'instance affectée. Ne créez pas d'instance Windows Server 2012 R2.

Important

Si vous ne créez pas l'instance dans la même zone de disponibilité que l'instance affectée, vous ne pourrez pas attacher le volume racine de celle-ci à la nouvelle instance.

5. Dans le panneau de navigation, choisissez Volumes.
6. Recherchez le volume racine de l'instance affectée. Détachez le volume et attachez-le à l'instance temporaire que vous avez créée précédemment. Attachez-le avec le nom du périphérique par défaut (xvdf).
7. Utilisez les services Bureau à distance pour vous connecter à l'instance temporaire, puis utilisez l'utilitaire Gestion des disques pour rendre le volume disponible.
8. Sur l'instance temporaire, ouvrez la boîte de dialogue Run (Exécuter), tapez **regedit** et appuyez sur Entrée.
9. Dans le volet de navigation de l'Editeur du Registre, choisissez HKEY_Local_Machine, puis dans le menu File (Fichier), choisissez Load Hive (Charger Hive).

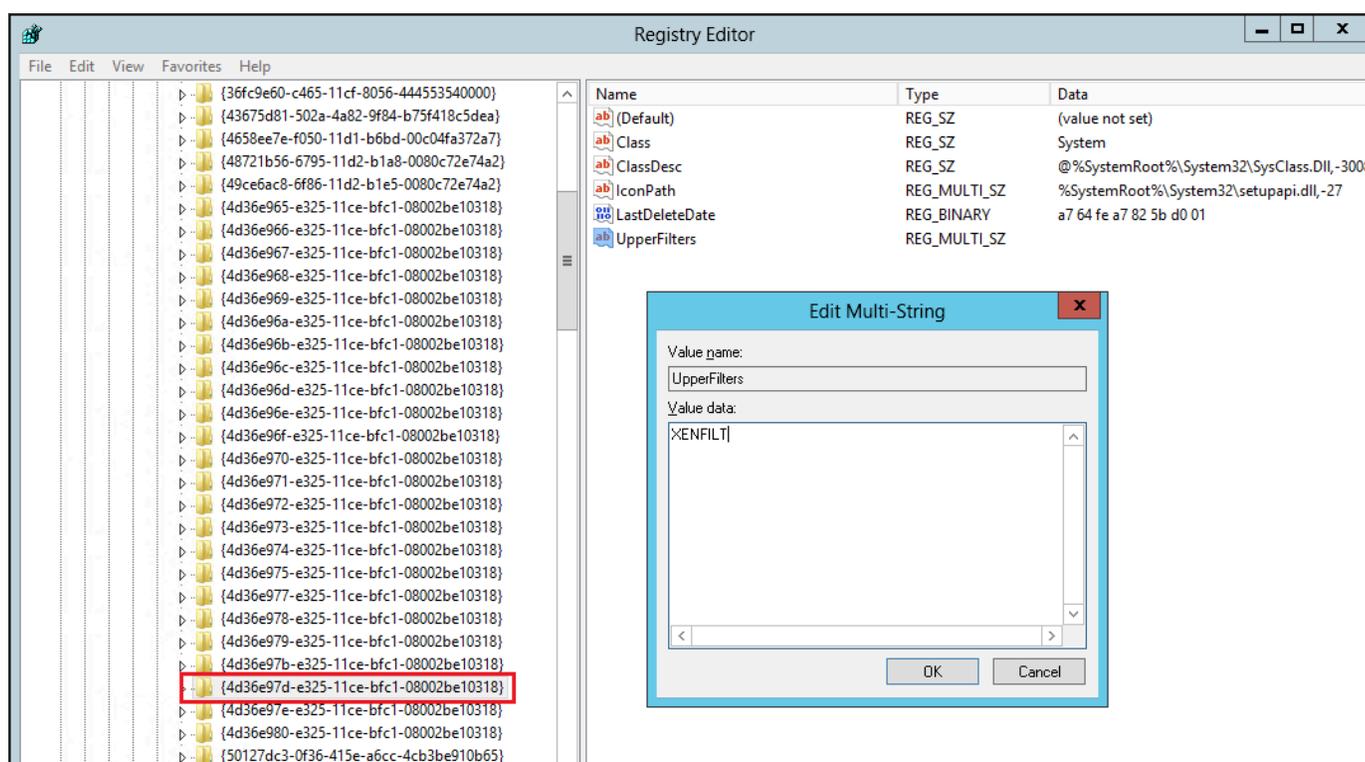
10. Dans la boîte de dialogue Load Hive (Charger Hive), accédez à Affected Volume (Volume affecté)\Windows\System32\config\System et tapez un nom temporaire dans la boîte de dialogue Key Name (Nom de la clé). Par exemple, saisissez OldSys.

11. Dans le volet de navigation de l'Éditeur du registre, recherchez les clés suivantes :

HKEY_LOCAL_MACHINE \ ***your_temporary_key_name*** \ 001 \ Control \ Class \ ***4d36e97d-e325-11ce-bfc1-08002be10318*** ControlSet

HKEY_LOCAL_MACHINE \ ***your_temporary_key_name*** \ 001 \ Control \ Class \ ***4d36e96a-e325-11ce-bfc1-08002be10318*** ControlSet

12. Pour chaque clé, double-cliquez UpperFilters, entrez la valeur XENFILT, puis cliquez sur OK.



13. Recherchez les clés suivantes :

HKEY_LOCAL_MACHINE \ ***your_temporary_key_name*** \ 001 \ Services \ XENBUS \ Paramètres ControlSet

14. Créez une nouvelle chaîne (REG_SZ) avec le nom ActiveDevice et la valeur suivants :

PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Recherchez les clés suivantes :

HKEY_LOCAL_MACHINE \ *votre_nom_clé_temporaire* \ 001 \ Services \ XENBUS
ControlSet

16. Remplacez la valeur Nombre de 0 à 1.

17. Recherchez et supprimez les clés suivantes :

HKEY_LOCAL_MACHINE \ *votre_nom_clé_temporaire* \ 001 \ Services \ xenvbd \
ControlSet StartOverride

HKEY_LOCAL_MACHINE \ *votre_nom_clé temporaire* \ 001 \ Services \
xenfilt \ ControlSet StartOverride

18. Dans le volet de navigation de l'Editeur du Registre, choisissez la clé temporaire que vous avez créée lorsque vous avez ouvert pour la première fois l'Editeur du Registre.

19. Dans le menu File (Fichier), choisissez Unload Hive (Décharger Hive).

20. Dans l'utilitaire Gestion des disques, choisissez le lecteur que vous avez attaché précédemment, ouvrez le menu contextuel (clic droit) et choisissez Hors connexion.

21. Dans la console Amazon EC2, détachez le volume affecté de l'instance temporaire et rattachez-le à votre instance Windows Server 2012 R2 avec le nom de périphérique /dev/sda1. Vous devez spécifier ce nom de périphérique pour désigner le volume en tant que volume racine.

22. [Démarrez](#) l'instance.

23. Connectez-vous à l'instance à l'aide de Remote Desktop, puis [téléchargez](#) le package AWS PV Drivers Upgrade sur l'instance.

24. Extrayez le contenu du dossier, puis exécutez AWSPVDriverSetup.msi.

Après avoir exécuté le MSI, l'instance redémarre automatiquement puis met à niveau les pilotes. L'instance ne sera pas disponible pendant 15 minutes.

25. Une fois la mise à niveau terminée et que l'instance réussit les deux vérifications de l'état dans la console Amazon EC2, connectez-vous à l'instance à l'aide des services Bureau à distance et vérifiez que les nouveaux pilotes ont été installés. Dans le Gestionnaire de périphériques, sous Contrôleurs de stockage, recherchez Carte hôte AWS PV Storage. Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez [AWS Historique du package de pilotes PV](#).

26. Supprimez ou arrêtez l'instance temporaire que vous avez créée au cours de cette procédure.

Exécuter le script de correction

Si vous ne pouvez pas exécuter une mise à niveau du pilote sur place ou migrer vers une instance plus récente, vous pouvez exécuter le script de correction pour corriger les problèmes causés par la tâche de nettoyage Plug and Play.

Pour exécuter le script de correction

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance pour laquelle vous souhaitez exécuter le script de correction. Sélectionnez État de l'instance, puis Arrêter l'instance.

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

4. Une fois l'instance arrêtée, créez une sauvegarde. Sélectionnez l'instance, puis Actions, Image et modèles et enfin Créer une image.
5. Sélectionnez État de l'instance, puis Démarrer l'instance.
6. Connectez-vous à l'instance à l'aide de Remote Desktop, puis [téléchargez](#) le dossier RemediateDriverIssue .zip sur l'instance.
7. Extrayez le contenu du dossier.
8. Exécutez le script de correction en fonction des instructions contenues dans le fichier Readme.txt. Le fichier se trouve dans le dossier dans lequel vous avez extrait le fichier RemediateDriverIssue .zip.

Transfert de la charge TCP

Important

Ce problème ne s'applique pas aux instances exécutant des pilotes réseau AWS PV ou Intel.

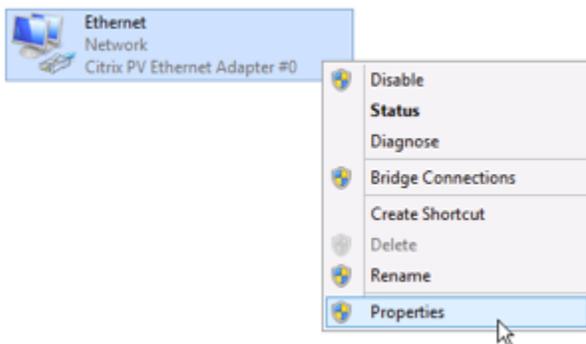
Par défaut, le transfert de la charge TCP est activé pour les pilotes PV Citrix dans les AMI Windows. Si vous rencontrez des problèmes au niveau du transport ou de la transmission de paquets (comme indiqué sur Windows Performance Monitor), par exemple, lorsque vous exécutez certaines charges de travail SQL, vous pouvez devoir désactiver cette fonction.

Warning

La désactivation du transfert de la charge TCP peut réduire les performances réseau de votre instance.

Pour désactiver le transfert de la charge TCP pour Windows Server 2012 et 2008

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Si vous utilisez Windows Server 2012, appuyez sur Ctrl+Échap pour accéder à l'écran Démarrer, puis cliquez sur Panneau de configuration. Si vous utilisez Windows Server 2008, cliquez sur Démarrer et sélectionnez Panneau de configuration.
3. Choisissez Réseau et Internet, puis Centre Réseau et partage.
4. Cliquez sur Modifier les paramètres de la carte.
5. Cliquez avec le bouton droit sur Carte Ethernet PV Citrix #0, puis cliquez sur Propriétés.



6. Dans la boîte de dialogue Propriétés de la connexion au réseau local, cliquez sur Configurer pour ouvrir la boîte de dialogue Propriétés de la carte Ethernet PV Citrix #0.
7. Sous l'onglet Advanced (Avancé), désactivez chacune des propriétés, à l'exception de Correct TCP/UDP Checksum Value (Corriger la valeur de la somme de contrôle TCP/UDP). Pour désactiver une propriété, sélectionnez-la dans Property (Propriété) et choisissez Disabled (Désactivé) dans Value (Valeur).
8. Choisissez OK.
9. A partir d'une fenêtre d'invite de commande, exécutez les commandes suivantes :

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Redémarrez l'instance.

Synchronisation du temps

Avant l'édition du 13/02/2013 de l'AMI Windows, l'agent invité Citrix Xen pouvait définir l'heure de manière incorrecte. Cela peut entraîner l'expiration du bail DHCP. En cas de problème pour vous connecter à votre instance, vous pouvez avoir besoin de mettre à niveau l'agent.

Pour déterminer si vous avez l'agent invité Citrix Xen mis à jour, vérifiez que le fichier `C:\Program Files\Citrix\XenGuestAgent.exe` date de mars 2013. Si la date sur le fichier est antérieure, mettez à jour le service d'agent invité Citrix Xen. Pour plus d'informations, consultez [Mettre à niveau votre service d'agent invité Citrix Xen](#).

Les charges de travail qui exploitent plus de 20 000 IOPS disque subissent une dégradation due aux goulots d'étranglement du processeur

Vous pouvez être affecté par ce problème si vous utilisez des instances Windows exécutant des pilotes PV AWS qui exploitent plus de 20 000 IOPS et que vous rencontrez un code de vérification des bogues `0x9E: USER_MODE_HEALTH_MONITOR`.

Les lectures et écritures sur disque (iOS) dans les pilotes AWS PV se déroulent en deux phases : préparation des E/S et achèvement des E/S. Par défaut, la phase de préparation s'exécute sur un cœur arbitraire unique. La phase d'achèvement s'exécute sur le cœur 0. La quantité de calcul requise pour traiter une opération d'IO varie en fonction de sa taille et d'autres propriétés. Certaines opération d'IO utilisent plus de calcul dans la phase de préparation, et d'autres dans la phase d'achèvement. Lorsqu'une instance gère plus de 20 000 IOPS, la phase de préparation ou d'achèvement peut entraîner un goulot d'étranglement, lorsque le processeur sur lequel elle s'exécute est à 100 % de sa capacité. Le fait que la phase de préparation ou d'achèvement provoque ou non un goulot d'étranglement dépend des propriétés des IO utilisée par l'application.

À partir de la version 8.4.0 des pilotes AWS photovoltaïques, la charge de la phase de préparation et de la phase d'achèvement peut être répartie sur plusieurs cœurs, éliminant ainsi les goulots d'étranglement. Chaque application utilise des propriétés d'IO différentes. Par conséquent,

l'application de l'une des configurations suivantes peut augmenter, diminuer ou ne pas affecter les performances de votre application. Après avoir appliqué l'une de ces configurations, surveillez l'application pour vérifier qu'elle enregistre les performances souhaitées.

1. Prérequis

Avant de commencer cette procédure de dépannage, vérifiez que les prérequis suivants sont respectés :

- Votre instance utilise des pilotes AWS PV version 8.4.0 ou ultérieure. Pour effectuer une mise à niveau, consultez [Mise à niveau des pilotes PV sur les instances Windows](#).
- Vous disposez d'un accès RDP à l'instance. Pour vous connecter à votre instance Windows à l'aide de RDP, consultez [Connectez-vous à votre instance Windows à l'aide d'un client RDP](#).
- Vous disposez d'un accès administrateur à l'instance.

2. Observer la charge processeur sur votre instance

Vous pouvez utiliser le Gestionnaire des tâches Windows pour afficher la charge sur chaque processeur afin de déterminer les goulots d'étranglement potentiels pour les IO disque.

1. Vérifiez que votre application est en cours d'exécution et gère un trafic similaire à votre charge de travail de production.
2. Connectez-vous à votre instance à l'aide de RDP.
3. Accédez menu Start (Démarrer) de votre instance.
4. Saisissez Task Manager dans le menu Start (Démarrer) pour ouvrir le Gestionnaire des tâches.
5. Si le Gestionnaire des tâches affiche la vue récapitulative, choisissez More details (Plus de détails) pour développer la vue détaillée.
6. Sélectionnez l'onglet Performance.
7. Sélectionner CPU (processeur) dans le volet gauche.
8. Cliquez avec le bouton droit de la souris sur le graphique dans le volet principal et sélectionnez Change graph to Logical processors (Changer le graphique en > processeurs logiques) pour afficher chaque cœur individuel.
9. Selon le nombre de cœurs sur votre instance, vous pouvez voir des lignes affichant la charge processeur au fil du temps, ou vous pouvez simplement voir un nombre.
 - Si vous voyez des graphiques affichant la charge dans le temps, recherchez les processeurs où la boîte est presque entièrement ombrée.

- Si vous voyez un nombre sur chaque cœur, recherchez les cœurs qui affichent systématiquement 95 % ou plus.

10 Notez si le cœur 0 ou un autre cœur subit une charge lourde.

3. Choisir la configuration à appliquer

Nom de la configuration	Quand appliquer cette configuration	Remarques
Default configuration	La charge de travail entraîne moins de 20 000 IOPS, ou d'autres configurations n'ont pas amélioré les performances ou la stabilité.	Pour cette configuration, les IO se produisent sur quelques cœurs, ce qui peut bénéficier à des charges de travail plus petites en augmentant la localité du cache et en réduisant le basculement de contexte.
Allow driver to choose whether to distribute completion	La charge de travail entraîne plus de 20 000 IOPS et une charge modérée ou élevée est observée sur le cœur 0.	Cette configuration est recommandée pour toutes les instances Xen utilisant PV 8.4.0 ou une version ultérieure et exploitant de plus de 20 000 IOPS, que des problèmes soient rencontrés ou non.
Distribute both preparation and completion	La charge de travail entraîne plus de 20 000 IOPS, et soit permettre au pilote de choisir la distribution n'a pas amélioré les performances, soit un cœur autre que 0 connaît une charge élevée.	Cette configuration permet la distribution à la fois de la préparation et de l'achèvement des IO.

Note

Nous vous recommandons de ne pas distribuer la préparation des IO sans distribuer également l'achèvement des IO (ne pas définir `DpcRedirection` sans définir `NotifierDistributed`), car la phase d'achèvement est sensible à la surcharge par la phase de préparation lorsque la phase de préparation est exécutée en parallèle.

Valeurs clés de registre

- `NotifierDistributed`

Valeur 0 ou aucune valeur — La phase d'achèvement se déroulera sur le cœur 0.

Valeur 1 — Le pilote choisit d'exécuter la phase d'achèvement sur le cœur 0 ou sur un cœur supplémentaire par disque connecté.

Valeur 2 — Le pilote exécute la phase d'achèvement sur un cœur supplémentaire par disque connecté.

- `DpcRedirection`

Valeur 0 ou aucune valeur — La phase de préparation se déroulera sur un cœur unique et arbitraire.

Valeur 1 — La phase de préparation est répartie sur plusieurs cœurs.

Configuration par défaut

Appliquez la configuration par défaut avec les versions du pilote AWS PV antérieures à la version 8.4.0, ou si une dégradation des performances ou de la stabilité est observée après l'application de l'une des autres configurations de cette section.

1. Connectez-vous à votre instance à l'aide de RDP.
2. Ouvrez une nouvelle invite de PowerShell commande en tant qu'administrateur.

3. Exécutez les commandes suivantes pour supprimer les clés de registre `NotifierDistributed` et `DpcRedirection`.

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name NotifierDistributed
```

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name DpcRedirection
```

4. Redémarrez votre instance.

Autoriser le pilote à choisir s'il doit distribuer l'achèvement

Définissez la clé de registre `NotifierDistributed` pour permettre au pilote de stockage PV de choisir de distribuer ou non l'achèvement des IO.

1. Connectez-vous à votre instance à l'aide de RDP.
2. Ouvrez une nouvelle invite de PowerShell commande en tant qu'administrateur.
3. Exécutez la commande suivante pour ajouter la clé de registre `NotifierDistributed`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Redémarrez votre instance.

Distribuer la préparation et l'achèvement

Définissez les clés de registre `NotifierDistributed` et `DpcRedirection` pour toujours distribuer les phases de préparation et d'achèvement.

1. Connectez-vous à votre instance à l'aide de RDP.
2. Ouvrez une nouvelle invite de PowerShell commande en tant qu'administrateur.
3. Exécutez les commandes suivantes pour définir les clés de registre `NotifierDistributed` et `DpcRedirection`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Redémarrez votre instance.

AWS Pilotes NVMe pour instances Windows

Les volumes Amazon EBS et les volumes de stockage d'instances sont exposés sous forme de blocs NVMe sur des [instances basées sur le système AWS Nitro](#). Pour utiliser pleinement les performances et les fonctionnalités d'Amazon EBS pour les volumes exposés sous forme de périphériques NVMe en mode bloc, le pilote AWS NVMe doit être installé sur l'instance. Le pilote AWS NVMe est installé par défaut sur toutes les AMI AWS Windows de dernière génération.

Pour plus d'informations sur EBS et NVMe, consultez [Amazon EBS et NVMe dans le guide de l'utilisateur](#) Amazon EBS. Pour plus d'informations sur le stockage d'instances SSD et sur NVMe, consultez [Volumes de stockage d'instance SSD](#).

Installez ou mettez à niveau les pilotes AWS NVMe à l'aide de PowerShell

Si vous n'utilisez pas les dernières AMI AWS Windows fournies par Amazon, suivez la procédure suivante pour installer le pilote AWS NVMe actuel. Vous devez effectuer cette mise à jour à un moment où il est possible de redémarrer votre instance. Soit le script d'installation redémarre votre instance, soit vous la redémarrez à l'étape finale.

Prérequis

PowerShell 3.0 ou version ultérieure

Pour télécharger et installer le dernier pilote AWS NVMe

1. Nous vous recommandons de créer une AMI en tant que sauvegarde comme suit, au cas où vous auriez besoin d'annuler vos modifications.
 - a. Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Avant d'arrêter une instance, vérifiez que vous avez copié toutes

les données dont vous avez besoin à partir de vos volumes de stockage d'instances vers un stockage persistant, tel que Amazon EBS ou Amazon S3.

- b. Dans le panneau de navigation, choisissez Instances.
 - c. Sélectionnez l'instance qui nécessite la mise à niveau du pilote, puis État de l'instance, Arrêter l'instance.
 - d. Une fois l'instance arrêtée, sélectionnez l'instance, puis Actions, Image et modèles, et enfin Créer une image.
 - e. Choisissez État de l'instance, Démarrer l'instance.
2. Connectez-vous à votre instance en tant qu'administrateur local.
 3. Téléchargez et extrayez les pilotes vers votre instance à l'aide de l'une des options suivantes :
 - Avec un navigateur :
 - a. [Téléchargez](#) le package de pilotes le plus récent sur l'instance.
 - b. Décompressez l'archive zip.
 - En utilisant PowerShell :

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
$env:userprofile\nvme_driver
```

Note

Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que le protocole TLS 1.2 doive être activé sur votre PowerShell terminal. Vous pouvez activer le protocole TLS 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
```

4. Installez le pilote sur votre instance en exécutant le `install.ps1` PowerShell script depuis le `nvme_driver` répertoire (`.\install.ps1`). Si un message d'erreur s'affiche, assurez-vous que vous utilisez la PowerShell version 3.0 ou une version ultérieure.

- a. (Facultatif) À partir de la version AWS NVMe1.5.0, les réservations persistantes SCSI (Small Computer System Interface) sont prises en charge pour Windows Server 2016 et versions ultérieures. Cette fonctionnalité ajoute la prise en charge du clustering de basculement Windows Server avec un stockage Amazon EBS partagé. Par défaut, cette fonctionnalité n'est pas activée lors de l'installation.

Vous pouvez désactiver cette fonctionnalité lors de l'exécution du script `install.ps1` pour installer le pilote en spécifiant le paramètre `EnableSCSIPersistentReservations` avec une valeur de `$true`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
```

Vous pouvez désactiver cette fonctionnalité lors de l'exécution du script `install.ps1` pour installer le pilote en spécifiant le paramètre `EnableSCSIPersistentReservations` avec une valeur de `$false`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
```

- b. À partir de AWS NVMe1.5.0, le `install.ps1` script installe toujours l'`ebsnvme-id` outil avec le pilote.

(Facultatif) Pour les versions 1.4.0, 1.4.1 et 1.4.2, le script `install.ps1` vous permet de spécifier si l'outil `ebsnvme-id` doit être installé avec le pilote.

- i. Pour installer l'outil `ebsnvme-id`, spécifiez `InstallEBSNVMeIdTool 'Yes'`.
- ii. Si vous ne souhaitez pas installer l'outil, spécifiez `InstallEBSNVMeIdTool 'No'`.

Si vous ne spécifiez pas `InstallEBSNVMeIdTool` et que l'outil est déjà présent sur `C:\ProgramData\Amazon\Tools`, le package met à niveau l'outil par défaut. Si l'outil n'est pas présent, `install.ps1` ne mettra pas à niveau l'outil par défaut.

Si vous ne souhaitez pas installer l'outil dans le package, mais que vous souhaitez l'installer ultérieurement, vous trouverez la dernière version ou l'outil dans le package du pilote. Vous pouvez également télécharger la version 1.0.0 depuis Amazon S3 :

[Téléchargez](#) l'outil `ebsnvme-id`.

5. Si le programme d'installation ne redémarre pas votre instance, procédez vous-même au redémarrage.

Installation ou mise à niveau des pilotes AWS NVMe avec le distributeur

Vous pouvez utiliser Distributor, une fonctionnalité de AWS Systems Manager, pour installer le package de pilotes NVMe une fois ou avec des mises à jour planifiées.

1. Pour obtenir les instructions sur l'installation du package de pilotes NVMe à l'aide de Distributor, reportez-vous aux procédures de la section [Installer ou mettre à jour des packages](#) dans le Guide de l'utilisateur Amazon EC2 Systems Manager.
2. Dans Nom, choisissez AWSNVMe.
3. Pour le type d'installation, sélectionnez Désinstaller et réinstallez.
4. (Facultatif) Personnalisez l'installation en spécifiant des valeurs pour `AdditionalArguments`.
 - a. À partir de AWS NVMe1.5.0, le pilote prend en charge les réservations persistantes SCSI pour Windows Server 2016 et versions ultérieures. Par défaut, cette fonctionnalité n'est pas activée lors de l'installation. Pour activer cette fonctionnalité, spécifiez `{"SSM_EnableSCSIPersistentReservations": $true}` pour `AdditionalArguments`. Si vous ne souhaitez pas activer cette fonctionnalité, spécifiez `{"SSM_EnableSCSIPersistentReservations": $false}` pour `AdditionalArguments`.
 - b. À partir de AWS NVMe1.5.0, le `install.ps1` script installera toujours l'`ebsnvme-idoutil`.

(Facultatif) Pour les versions 1.4.0, 1.4.1 et 1.4.2, le script `install.ps1` vous permet de spécifier si l'outil `ebsnvme-id` doit être installé avec le pilote.

 - i. Pour installer l'outil `ebsnvme-id`, spécifiez `{"SSM_InstallEBSNVMeIdTool": "Yes"}` pour `AdditionalArguments`.
 - ii. Si vous ne souhaitez pas installer l'outil, spécifiez `{"SSM_InstallEBSNVMeIdTool": "No"}` pour `AdditionalArguments`.

Si `SSM_InstallEBSNVMeIdTool` n'est pas spécifié pour `AdditionalArguments` et que l'outil est déjà présent sur `C:\ProgramData\Amazon\Tools`, le package met à niveau l'outil par défaut. Si l'outil n'est pas présent, le package ne mettra pas à niveau l'outil par défaut. La commande `Addition arguments` (Arguments supplémentaires) doit être formatée à l'aide de la syntaxe JSON valide. Pour obtenir des exemples de passage d'arguments supplémentaires pour le package `aws configure`, consultez la [documentation Amazon EC2 Systems Manager](#).

Si vous ne souhaitez pas installer l'outil dans le package, mais que vous souhaitez l'installer ultérieurement, vous trouverez la dernière version ou l'outil dans le package du pilote. Vous pouvez également télécharger la version 1.0.0 depuis Amazon S3 :

[Téléchargez](#) l'outil `ebsnvme-id`.

5. Si le programme d'installation ne redémarre pas votre instance, procédez vous-même au redémarrage.

Configurer les réservations persistantes SCSI

Une fois la version du pilote AWS NVMe 1.5.0 ou ultérieure installée, vous pouvez activer ou désactiver les réservations persistantes SCSI à l'aide du registre Windows pour Windows Server 2016 et versions ultérieures. Vous devez redémarrer l'instance pour que les modifications du registre prennent effet.

Vous pouvez activer les réservations persistantes SCSI à l'aide de la commande suivante qui définit `EnableSCSIPersistentReservations` sur 1.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters\nDevice"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

Vous pouvez désactiver les réservations persistantes SCSI à l'aide de la commande suivante qui définit 0 sur `EnableSCSIPersistentReservations`.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters\nDevice"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

AWS Historique des versions du pilote NVMe

Le tableau suivant décrit les versions publiées du pilote AWS NVMe.

Version du package	Versions du pilote	Détails	Date de publication
1.5.1	1.5.0	Correction du script d'installation permettant de créer un dossier pour l'outil ebsnvme-id s'il n'est pas présent.	17 novembre 2023
1.5.0	1.5.0	Ajout de la prise en charge des réservations persistantes SCSI (Small Computer System Interface) pour les instances exécutant Windows Server 2016 et versions ultérieures. L'outil ebsnvme-id (ebsnvme-id.exe) est désormais installé par défaut.	31 août 2023
1.4.2	1.4.2	Correction d'un bogue qui Pilote AWS NVMe empêchait les volumes de stockage d'instance sur les instances D3.	16 mars 2023
1.4.1	1.4.1	Indique la granularité d'écriture préférée d'espace de noms (NPGW, Namespace Preferred Write Granularity) pour les volumes EBS qui prennent en charge cette fonction NVMe facultative. Pour plus d'informations, reportez-vous à la section 8.25, « Amélioration des performances grâce à la taille des I/O et à l'adhérence de l'alignement », dans la rubrique Spécification de base NVMe, version 1.4 .	20 mai 2022
1.4.0	1.4.0	<ul style="list-style-type: none"> Ajout de la prise en charge des IOCTL qui permettent aux applications d'interagir avec les dispositifs NVMe. Cette prise en charge permet aux applications d'obtenir une liste de <code>IdentifyController</code>, <code>IdentifyNamespace</code> et <code>NameSpace</code> à partir du dispositif NVMe. Pour plus d'informations, consultez Requêtes spécifiques au protocole dans la documentation Microsoft. AWSNVMe L'installation de la version 1.4.0 sur Windows Server 2008 R2 échouera. AWSNVMe les 	23 novembre 2021

Version du package	Versions du pilote	Détails	Date de publication
		<p>versions 1.3.2 et antérieures sont prises en charge sur Windows Server 2008 R2.</p> <ul style="list-style-type: none"> La version 1.4.0 du pilote et le dernier outil <code>ebsnvme-id</code> (<code>ebsnvme-id.exe</code>) sont combinés dans un seul package. Cette combinaison vous permet d'installer à la fois le pilote et l'outil à partir d'un seul package. Pour en savoir plus, consultez Installez ou mettez à niveau les pilotes AWS NVMe à l'aide de PowerShell. Correctifs de bogues et améliorations de fiabilité. 	
1.3.2	1.3.2	Résolution du problème de modification des volumes EBS traitant activement des I/O, qui pouvait entraîner une altération des données. Les clients qui ne modifient pas les volumes EBS en ligne (par exemple, en les redimensionnant ou en changeant de type) ne sont pas concernés.	10 septembre 2019
1.3.1	1.3.1	Améliorations de la fiabilité.	21 mai 2019
1.3.0	1.3.0	Améliorations de l'optimisation des appareils.	31 août 2018
1.2.0	1.2.0	Améliorations des performances et de la fiabilité des appareils AWS NVMe sur toutes les instances prises en charge, y compris les instances bare metal.	13 juin 2018
1.0.0	1.0.0	AWS Pilote NVMe pour les types d'instances pris en charge exécutant Windows Server.	12 février 2018

S'abonner aux notifications

Amazon SNS peut vous notifier en cas de publication de nouvelles versions des pilotes Windows EC2. Pour vous abonner à ces notifications, utilisez la procédure suivante.

Pour vous abonner aux notifications EC2 à partir de la console

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région, car les notifications SNS auxquelles vous vous abonnez sont dans cette région.
3. Dans le panneau de navigation, choisissez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :
 - a. Pour TopicARN, copiez l'Amazon Resource Name (ARN) suivant :
`arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers`
 - b. Pour Protocole, choisissez Email.
 - c. Pour Point de terminaison, tapez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications.
 - d. Choisissez Créer un abonnement.
6. Vous recevrez rapidement un e-mail de confirmation. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Chaque fois que des pilotes Windows EC2 sont publiés, nous envoyons des notifications aux abonnés de la rubrique . Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Pour se désinscrire des notifications des pilotes Windows Amazon EC2

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans le panneau de navigation, choisissez Abonnements.

3. Cochez la case correspondant à l'abonnement, puis choisissez Actions, Supprimer des abonnements. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour vous abonner aux notifications EC2 à l'aide du AWS CLI

Pour vous abonner aux notifications EC2 avec le AWS CLI, utilisez la commande suivante.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --  
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Pour vous abonner aux notifications EC2 à l'aide de AWS Tools for Windows PowerShell

Pour vous abonner aux notifications EC2 avec AWS Tools for Windows PowerShell, utilisez la commande suivante.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-  
drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Configurer votre instance Windows

Après avoir lancé une instance Windows, vous pouvez vous connecter en tant qu'administrateur pour effectuer une configuration supplémentaire pour les agents de lancement et les fonctionnalités spécifiques à Windows. Les rubriques suivantes portent sur la configuration des instances Windows.

Table des matières

- [Configuration des paramètres de lancement pour les instances Windows Amazon EC2](#)
- [Utilisez EC2 Fast Launch pour vos instances Windows](#)
- [Utiliser les accélérateurs Amazon Elastic Graphics sur les instances Windows](#)
- [Installation de WSL sur votre instance Windows](#)

Configuration des paramètres de lancement pour les instances Windows Amazon EC2

Les agents de lancement Amazon EC2 exécutent des tâches lors du démarrage de l'instance et s'exécutent si une instance est arrêtée puis démarrée ou redémarrée ultérieurement. Pour plus d'informations sur un agent spécifique, consultez les pages détaillées de la liste suivante.

- [Configurer une instance Windows à l'aide d'EC2Launch v2](#)
- [Configurer une instance Windows à l'aide d'EC2Launch](#)
- [Configuration d'une instance Windows à l'aide du service EC2Config \(ancien\)](#)

Contenu

- [Comparez les agents de lancement Amazon EC2](#)
- [Configurer le suffixe DNS pour les agents de lancement Windows](#)

Comparez les agents de lancement Amazon EC2

Le tableau suivant présente les principales différences fonctionnelles entre EC2Config, EC2Launch v1 et EC2Launch v2.

Fonction	EC2Config	EC2Launch v1	EC2Launch v2
Exécuter en tant que	Windows Service	PowerShell Scripts	Windows Service
Prend en charge	Système d'exploitation hérité uniquement	Windows 2016 Windows 2019 (LTSC et SAC)	Windows 2016 Windows 2019 (LTSC et SAC) Windows 2022
Fichier de configuration	xml	xml	YAML
Définir le nom d'utilisateur de l'administrateur	Non	Non	Oui
Taille des données utilisateur	16 Ko	16 Ko	60 Ko (compressé)
Données utilisateur locales précalculées sur l'AMI	Non	Non	Oui, configurable

Fonction	EC2Config	EC2Launch v1	EC2Launch v2
Configuration de la tâche dans les données utilisateur	Non	Non	Oui
Fond d'écran configurable	Non	Non	Oui
Personnaliser l'ordre d'exécution des tâches	Non	Non	Oui
Tâches configurables	15	9	20 au lancement
Prend en charge l'Observateur d'événements Windows	Oui	Non	Oui
Nombre de types d'événements de l'Observateur d'événements	2	0	30

 Note

La documentation EC2Config est fournie à titre de référence historique uniquement. Les versions du système d'exploitation sur lesquelles il s'exécute ne sont plus prises en charge par Microsoft. Nous vous recommandons vivement de passer au dernier service de lancement.

Configurer le suffixe DNS pour les agents de lancement Windows

Avec les agents de lancement Amazon EC2, vous pouvez configurer une liste de suffixes DNS que les instances Windows utilisent pour la résolution des noms de domaine. Les agents de lancement remplacent les paramètres Windows standard de la clé de `System\CurrentControlSet`

\Services\Tcpip\Parameters\SearchList registre en ajoutant les valeurs suivantes à la liste de recherche des suffixes DNS :

- Le domaine de l'instance
- Les suffixes résultant de la dévolution du domaine d'instance
- Domaine NV
- Les domaines spécifiés par chaque carte d'interface réseau

Tous les agents de lancement prennent en charge la configuration des suffixes DNS. Pour plus d'informations, consultez la version de votre agent de lancement spécifique :

- Pour plus d'informations sur la `setDnsSuffix` tâche et sur la façon de configurer les suffixes DNS dans EC2Launch v2, consultez. [setDnsSuffix](#)
- Pour plus d'informations sur la configuration de la liste de suffixes DNS et sur la manière d'activer ou de désactiver la dévolution pour EC2Launch v1, consultez. [Configurer EC2Launch](#)
- Pour plus d'informations sur la configuration de la liste de suffixes DNS et sur la manière d'activer ou de désactiver la dévolution pour EC2Config, consultez. [Fichiers de paramètres EC2Config](#)

Dévolution des noms de domaine

La dévolution des noms de domaine est un comportement Active Directory qui permet aux ordinateurs d'un domaine enfant d'accéder aux ressources du domaine parent sans utiliser de nom de domaine complet. Par défaut, la dévolution des noms de domaine se poursuit jusqu'à ce qu'il ne reste que deux nœuds dans la progression des noms de domaine.

Les agents de lancement effectuent la dévolution du nom de domaine si l'instance est connectée à un domaine et ajoutent les résultats à la liste de recherche de suffixes DNS conservée dans la clé de **System\CurrentControlSet\Services\Tcpip\Parameters\SearchList** registre. Les agents utilisent les paramètres des clés de registre suivantes pour déterminer le comportement de dévolution.

- **System\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution**
 - Lorsqu'il n'est pas défini, désactive la dévolution
 - Lorsqu'il est défini sur 1, active la dévolution (par défaut)
 - Lorsque ce paramètre est défini sur 0, désactive la dévolution

- **System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel**

- Lorsqu'il n'est pas défini, utilisez le niveau de 2 (par défaut)
- Lorsque le paramètre est réglé sur 3 ou supérieur, utilisez la valeur pour définir le niveau

Lorsque vous désactivez la dévolution ou que vous modifiez vos paramètres de dévolution à un niveau supérieur, la clé de System\CurrentControlSet\Services\Tcpip\Parameters\SearchList registre contient toujours les suffixes ajoutés précédemment. Ils ne sont pas automatiquement supprimés. Vous pouvez mettre à jour la liste manuellement ou effacer la liste et laisser votre agent suivre le processus de configuration de la nouvelle liste.

 Note

Pour effacer la liste des suffixes DNS du registre, vous pouvez exécuter la commande suivante.

```
PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -  
Methodname "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =  
$null } | Out-Null
```

Exemples de transfert de responsabilités

Les exemples suivants montrent la progression des noms de domaine tout au long du processus de dévolution.

corp.example.com

- Procède à example.com

locale.region.corp.example.com

1. Procède à region.corp.example.com
2. Procède à corp.example.com
3. Procède à example.com

`locale.region.corp.example.com` avec un réglage de `DomainNameDevolutionLevel=3`

1. Procède à `region.corp.example.com`
2. Progresses vers `corp.example.com`. La progression s'arrête là, en raison du réglage du niveau.

Configurer une instance Windows à l'aide d'EC2Launch v2

Toutes les instances prises en charge d'Amazon EC2 exécutant Windows Server 2022 incluent l'agent de lancement EC2Launch v2 (`EC2Launch.exe`) par défaut. Nous fournissons également des AMI Windows Server 2016 et 2019 avec EC2Launch v2 installé comme agent de lancement par défaut. Ces AMI sont fournies en plus des AMI Windows Server 2016 et 2019 qui incluent EC2Launch v1. Vous pouvez rechercher les AMI Windows qui incluent EC2Launch v2 par défaut en saisissant le préfixe suivant dans votre recherche depuis la page AMIs de la console Amazon EC2 : `EC2LaunchV2-Windows_Server-*`.

EC2Launch v2 est un service qui effectue des tâches pendant le démarrage de l'instance et s'exécute si une instance est arrêtée et démarrée ultérieurement, ou redémarrée. EC2Launch v2 peut également effectuer des tâches à la demande. Certaines de ces tâches sont automatiquement activées, alors que d'autres doivent être activées manuellement. Le service EC2Launch v2 prend en charge toutes les fonctionnalités EC2Config et EC2Launch.

Ce service utilise un fichier de configuration pour contrôler son fonctionnement. Vous pouvez mettre à jour le fichier de configuration à l'aide d'un outil graphique ou en le modifiant directement en tant que fichier `.yml` unique (`agent-config.yml`). Les binaires de service se trouvent dans le répertoire `%ProgramFiles%\Amazon\EC2Launch`.

EC2Launch v2 publie les journaux d'événements Windows pour vous aider à résoudre les erreurs et à définir des déclencheurs. Pour plus d'informations, consultez [Journaux d'événements Windows](#).

Systèmes d'exploitation pris en charge

- Windows Server 2022
- Windows Server 2019 (canal de maintenance à long terme et canal semestriel)
- Windows Server 2016

Contenu de la section EC2Launch v2

- [Présentation d'EC2Launch v2](#)

- [Installer la version la plus récente d'EC2Launch v2](#)
- [Migrer vers EC2Launch v2](#)
- [Arrêter, redémarrer, supprimer ou désinstaller EC2Launch v2](#)
- [S'abonner aux notifications du service EC2Launch v2](#)
- [Paramètres EC2Launch v2](#)
- [Dépannage d'EC2Launch v2](#)
- [Historique des versions EC2Launch v2](#)

Présentation d'EC2Launch v2

EC2Launch v2 est un service qui effectue des tâches pendant le démarrage de l'instance et s'exécute si une instance est arrêtée et démarrée ultérieurement, ou redémarrée.

Sujets d'ensemble

- [Concepts EC2Launch v2](#)
- [Tâches EC2Launch v2](#)
- [Télémétrie](#)

Pour comparer les fonctionnalités des versions de l'agent de lancement, voir [Comparez les agents de lancement Amazon EC2](#).

Concepts EC2Launch v2

Les concepts suivants sont utiles à comprendre lors de l'étude de EC2Launch v2.

Tâche

Vous pouvez invoquer une tâche pour effectuer une action sur une instance. Vous pouvez configurer les tâches dans le fichier `agent-config.yml` ou via les données utilisateur. Pour consulter la liste des tâches disponibles pour EC2Launch v2, consultez [Tâches EC2Launch v2](#). Pour le schéma de configuration des tâches et les détails, consultez [Configuration de tâche EC2Launch v2](#).

Étape

Une étape est un regroupement logique de tâches que l'agent EC2Launch v2 exécute. Certaines tâches ne peuvent s'exécuter qu'à un stade spécifique. D'autres peuvent fonctionner en plusieurs étapes. Lors de l'utilisation de `agent-config.yml`, vous devez spécifier une liste d'étapes et une liste de tâches à exécuter au sein de chaque étape.

Le service exécute les étapes dans l'ordre suivant :

Étape 1 : Démarrage

Étape 2 : Réseau

Étape 3 : PreReady

Windows est prêt

Une fois l' PreReady étape terminée, le service envoie le `Windows is ready` message à la console Amazon EC2.

Étape 4 : PostReady

Les données utilisateur sont exécutées pendant la PostReadyphase. Certaines versions de script s'exécutent avant le PostReadystage du `agent-config.yml` fichier, tandis que d'autres s'exécutent après, comme suit :

Avant `agent-config.yml`

- Données utilisateur YAML version 1.1
- Données utilisateur XML

Après `agent-config.yml`

- Données utilisateur YAML version 1.0 (ancienne version pour la rétrocompatibilité)

Pour des exemples d'étapes et de tâches, consultez [Exemple : agent-config.yml](#).

Lorsque vous utilisez des données utilisateur, vous devez spécifier une liste de tâches que l'agent de lancement doit exécuter. L'étape est implicite. Pour des exemples de tâches, consultez [Exemple : données utilisateur](#).

EC2Launch v2 exécute la liste des tâches dans l'ordre que vous spécifiez dans `agent-config.yml` et dans les données utilisateur. Les étapes s'exécutent de manière séquentielle. L'étape suivante commence lorsque l'étape précédente est terminée. Les tâches sont également exécutées de manière séquentielle.

Fréquence

La fréquence des tâches détermine le moment où les tâches doivent être exécutées, en fonction du contexte de démarrage. La plupart des tâches n'ont qu'une seule fréquence autorisée. Vous pouvez spécifier une fréquence pour les tâches `executeScript`.

Vous verrez les fréquences suivantes dans la [Configuration de tâche EC2Launch v2](#).

- Une fois : la tâche s'exécute une fois, lorsque l'AMI démarre pour la première fois (Sysprep terminé).
- Toujours : la tâche s'exécute chaque fois que l'agent de lancement s'exécute. L'agent de lancement s'exécute lorsque :
 - une instance démarre ou redémarre
 - le service EC2Launch s'exécute
 - EC2Launch.exe run est invoqué

agent-config

agent-config est un fichier qui se trouve dans le dossier de configuration pour EC2Launch v2. Il inclut la configuration du démarrage PreReady, du réseau et des PostReady stages. Ce fichier est utilisé pour spécifier la configuration de l'instance pour les tâches qui doivent s'exécuter lorsque l'AMI est démarrée pour la première fois ou pour les fois suivantes.

Par défaut, l'installation EC2Launch v2 installe un fichier agent-config contenant les configurations recommandées qui sont utilisées dans les AMI Amazon Windows standard. Vous pouvez mettre à jour le fichier de configuration pour modifier l'expérience de démarrage par défaut de votre AMI que EC2Launch v2 spécifie.

Données utilisateur

Les données utilisateur sont des données configurables lorsque vous lancez une instance. Vous pouvez mettre à jour les données utilisateur pour modifier dynamiquement la configuration des AMI personnalisées ou des AMI de démarrage rapide. EC2Launch v2 prend en charge une longueur d'entrée des données utilisateur de 60 Ko. Les données utilisateur incluent uniquement l' UserData étape et s'exécutent donc après le agent-config fichier. Vous pouvez entrer des données utilisateur lorsque vous lancez une instance à l'aide de l'assistant de lancement d'instance, ou vous pouvez modifier les données utilisateur à partir de la console EC2. Pour plus d'informations sur l'utilisation des données d'utilisateur, consultez [Comment Amazon EC2 gère les données utilisateur pour les instances Windows](#).

Tâches EC2Launch v2

EC2Launch v2 peut effectuer les tâches suivantes à chaque démarrage :

- Configurez un nouveau fond d'écran personnalisé qui rend des informations sur l'instance.

- Définissez les attributs du compte d'administrateur créé sur la machine locale.
- Ajoutez des suffixes DNS à la liste des suffixes de recherche. Seuls les suffixes qui n'existent pas déjà sont ajoutés à la liste.
- Définissez les lettres de lecteur pour les volumes supplémentaires et étendez-les pour utiliser l'espace disponible.
- Ecrivez les fichiers de configuration sur le disque.
- Exécutez les scripts spécifiés dans le fichier de configuration EC2Launch v2 ou à partir de `user-data`. Les scripts de `user-data` peuvent être en texte brut ou compressés et fournis au format base64.
- Exécutez un programme avec des arguments donnés.
- Définir le nom d'ordinateur
- Envoyez des informations d'instance à la console Amazon EC2.
- Envoyez l'empreinte numérique du certificat RDP à la console Amazon EC2.
- Étendez de manière dynamique la partition du système d'exploitation pour inclure l'espace non partitionné.
- Exécutez des données utilisateur. Pour plus d'informations sur la spécification de données utilisateur, consultez [Configuration de tâche EC2Launch v2](#).
- Définissez des routes non statiques permanentes pour atteindre le service de métadonnées et les serveurs AWS KMS .
- Définissez les partitions autres que le démarrage sur `mbr` ou `gpt`.
- Démarrez le service Systems Manager après Sysprep.
- Optimisez les paramètres ENA.
- Activez OpenSSH pour les versions ultérieures de Windows.
- Activez les trames Jumbo.
- Définissez Sysprep pour qu'il s'exécute avec EC2Launch v2.
- Publiez les journaux des événements Windows.

Télémétrie

La télémétrie est une information supplémentaire qui permet de mieux AWS comprendre vos besoins, de diagnostiquer les problèmes et de fournir des fonctionnalités pour améliorer votre expérience avec Services AWS

Version EC2Launch v2 2.0.592 et ultérieures collecte les données de télémétrie, comme les métriques d'utilisation et les erreurs. Ces données sont collectées à partir de l'instance Amazon EC2 sur laquelle s'exécute EC2Launch v2. Cela inclut toutes les AMI Windows détenues par AWS.

Les types de données télémétriques suivants sont collectés par EC2Launch v2 :

- Usage information (Informations d'utilisation) : commandes de l'agent, méthode d'installation et fréquence d'exécution planifiée.
- Erreurs et informations de diagnostic : codes d'erreur d'installation de l'agent, codes d'erreur d'exécution et piles d'appels d'erreur.

Exemples de données collectées :

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

La télémétrie est activée par défaut. Vous pouvez désactiver la collecte de données de télémétrie à tout moment. Si la télémétrie est activée, EC2Launch v2 envoie des données de télémétrie sans notifications supplémentaires au client.

Visibilité de la télémétrie

Lorsque la télémétrie est activée, elle apparaît dans la sortie de la console Amazon EC2 comme suit.

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Désactiver la télémétrie sur une instance

Pour désactiver la télémétrie pour une seule instance, vous pouvez définir une variable d'environnement système ou utiliser le MSI pour modifier l'installation.

Pour désactiver la télémétrie en paramétrant une variable d'environnement système, exécutez la commande suivante en tant qu'administrateur.

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Pour désactiver la télémétrie à l'aide du MSI, exécutez la commande suivante après avoir [téléchargé le MSI](#).

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Installer la version la plus récente d'EC2Launch v2

Vous pouvez utiliser l'une des méthodes suivantes pour installer l'agent EC2Launch v2 sur votre instance EC2 :

- Téléchargez l'agent depuis Amazon S3 et installez-le avec Windows PowerShell. Pour les URL de téléchargement, veuillez consulter la rubrique [Téléchargements d'EC2Launch v2 sur Amazon S3](#).
- Installez à partir d'un distributeur SSM.
- Installez à partir d'un composant EC2 Image Builder.
- Lancez votre instance depuis une AMI sur laquelle EC2Launch v2 est préinstallé.

Warning

AmazonEC2Launch.msi désinstalle les versions précédentes des services de lancement EC2, tels que EC2Launch (v1) et EC2Config.

Pour les étapes d'installation, sélectionnez l'onglet correspondant à votre méthode préférée.

Windows PowerShell

Pour installer la dernière version de l'agent EC2Launch v2 sous Windows PowerShell, procédez comme suit.

1. Créez votre répertoire local.

```
New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
```

2. Définissez l'URL de votre emplacement de téléchargement. Exécutez la commande suivante avec l'URL Amazon S3 que vous allez utiliser. Pour les URL de téléchargement, veuillez consulter la rubrique [Téléchargements d'EC2Launch v2 sur Amazon S3](#).

```
$Url = "Amazon S3 URL/AmazonEC2Launch.msi"
```

3. Utilisation de la commande combinée suivante pour télécharger et installer l'agent

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

Note

Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que le protocole TLS 1.2 doive être activé sur votre PowerShell terminal. Vous pouvez activer le protocole TLS 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
```

4. Pour vérifier l'installation, vérifiez que le fichier msi existe dans le répertoire EC2Launch v2 de votre instance (C:\ProgramData\Amazon\EC2Launch).

AWS Systems Manager Distributor

Pour configurer les mises à jour automatiques pour EC2Launch v2 avec AWS Systems Manager Quick Setup, voir [Installation et mise à jour automatiques avec le programme de configuration rapide du distributeur](#)

Vous pouvez également effectuer une installation unique du AWSEC2Launch-Agent package depuis le AWS Systems Manager distributeur. Pour obtenir des instructions sur l'installation d'un package à partir d'un distributeur Systems Manager, veuillez consulter la rubrique [Installer ou mettre à jour des packages](#) dans le Guide de l'utilisateur AWS Systems Manager .

EC2 Image Builder component

Vous pouvez installer le composant ec2launch-v2-windows lorsque vous créez une image personnalisée avec EC2 Image Builder. Pour obtenir des instructions sur la création d'une image personnalisée avec EC2 Image Builder, consultez [Création d'un pipeline d'images à l'aide de l'assistant de la console EC2 Image Builder](#) dans le Guide de l'utilisateur EC2 Image Builder.

AMI

EC2Launch v2 est préinstallé par défaut sur les AMI Windows Server 2022 et les AMI UEFI suivantes :

- Windows_Server-2022-English-Full-Base
- Windows_Server-2022-English-Core-Base
- AMI Windows Server 2022 avec toutes les autres langues
- AMI Windows Server 2022 avec SQL installée
- Windows_Server-2022-English-Core-EKS_Optimized

EC2Launch v2 est également préinstallé sur les AMI Windows Server suivants. Vous pouvez trouver ces AMI à partir de la console Amazon EC2, ou en utilisant le préfixe de recherche suivant : EC2LaunchV2- dans l' AWS CLI.

- EC2LaunchV2-Windows_Server-2019-English-Core-Base
- EC2LaunchV2-Windows_Server-2019-English-Full-Base
- EC2LaunchV2-Windows_Server-2016-English-Core-Base
- EC2LaunchV2-Windows_Server-2016-English-Full-Base
- EC2LaunchV2-Windows_Server-2012_R2_RTM-English-Full-Base
- EC2LaunchV2-Windows_Server-2012_RTM-English-Full-Base

Installation et mise à jour automatiques d'EC2Launch v2 avec le programme de configuration rapide du AWS Systems Manager distributeur

Avec AWS Systems Manager Distributor Quick Setup, vous pouvez configurer des mises à jour automatiques pour EC2Launch v2. Le processus suivant permet de configurer une association Systems Manager sur votre instance qui met automatiquement à jour l'agent EC2Launch v2 à une fréquence que vous spécifiez. L'association créée par le programme de configuration rapide du distributeur peut inclure des instances au sein d'une région Compte AWS et, ou des instances au sein d'une AWS organisation. Pour plus d'informations sur la configuration d'une organisation, voir [Tutoriel : Création et configuration d'une organisation](#) dans le Guide de AWS Organizations l'utilisateur.

Avant de commencer, assurez-vous que vos instances répondent à tous les prérequis.

Prérequis

Pour configurer les mises à jour automatiques avec Distributor Quick Setup, vos instances doivent répondre aux conditions préalables suivantes.

- Vous avez au moins une instance en cours d'exécution qui prend en charge EC2Launch v2. Consultez les systèmes d'exploitation pris en charge pour [EC2Launch v2](#).
- Vous avez effectué les tâches de configuration de Systems Manager sur vos instances. Pour plus d'informations, consultez la section [Configuration de Systems Manager](#) dans le guide de AWS Systems Manager l'utilisateur.
- EC2Launch v2 doit être le seul agent de lancement installé sur votre instance. Si plusieurs agents de lancement sont installés, la configuration de configuration rapide de votre distributeur échouera. Avant de configurer EC2Launch v2 avec une configuration rapide du distributeur, désinstallez les agents de lancement EC2Config ou EC2Launch v1, s'ils existent.

Configurer la configuration rapide du distributeur pour EC2Launch v2

Pour créer une configuration pour EC2Launch v2 avec Distributor Quick Setup, utilisez les paramètres suivants lorsque vous terminez les étapes de déploiement [du package Distributor](#) :

- Packages logiciels : agent Amazon EC2Launch v2.
- Fréquence de mise à jour : sélectionnez une fréquence dans la liste.
- Cibles : choisissez parmi les options de déploiement disponibles.

Pour vérifier l'état de votre configuration, accédez à l'onglet Configurations de configuration rapide de Systems Manager dans le AWS Management Console.

1. Ouvrez la AWS Systems Manager console à l'[adresse https://console.aws.amazon.com/systems-manager/](https://console.aws.amazon.com/systems-manager/).
2. Dans le panneau de navigation, choisissez Configuration rapide.
3. Dans l'onglet Configurations, sélectionnez la ligne associée à la configuration que vous avez créée. L'onglet Configurations répertorie vos configurations et inclut un résumé des principaux détails, tels que la région, le statut du déploiement et le statut de l'association.

Note

Le nom de l'association pour chaque configuration du distributeur EC2Launch v2 commence par le préfixe suivant : `AWS-QuickSetup-Distributor-EC2Launch-Agent-`

4. Pour afficher les détails, sélectionnez la configuration et choisissez Afficher les détails.

Pour plus d'informations et pour connaître les étapes de résolution des problèmes, consultez la section [Résolution des problèmes liés à la configuration rapide](#) dans le Guide de AWS Systems Manager l'utilisateur.

Téléchargements d'EC2Launch v2 sur Amazon S3

Pour installer la dernière version d'EC2Launch v2, téléchargez le programme d'installation à partir de l'un des emplacements suivants :

Note

Le lien d'installation 32 bits sera obsolète. Nous vous recommandons d'utiliser le lien d'installation 64 bits pour installer EC2Launch v2. Si vous avez besoin d'un agent de lancement 32 bits, utilisez [EC2Config](#).

- 64Bit — <https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi>
- 32Bit — <https://s3.amazonaws.com/amazon-ec2launch-v2/windows/386/latest/AmazonEC2Launch.msi>

Configuration des options d'installation

Lorsque vous installez ou mettez à niveau EC2Launch v2, vous pouvez configurer les options d'installation à l'aide de la boîte de dialogue d'installation d'EC2Launch v2 ou de la commande `msiexec` dans un shell de ligne de commande.

La première fois que le programme d'installation d'EC2Launch v2 s'exécute sur une instance, il initialise les paramètres de l'agent de lancement sur votre instance comme suit :

- Il crée le chemin local et y écrit le fichier de l'agent de lancement. C'est ce que l'on appelle parfois l'installation propre.
- Il crée la variable d'environnement `EC2LAUNCH_TELEMETRY` si elle n'existe pas déjà, et la définit en fonction de votre configuration.

Pour les détails de configuration, sélectionnez l'onglet correspondant à la méthode de configuration que vous allez utiliser.

Amazon EC2Launch Setup dialog

Lorsque vous installez ou mettez à niveau EC2Launch v2, vous pouvez configurer les options d'installation suivantes à l'aide de la boîte de dialogue d'installation d'EC2Launch v2.

Options d'installation de base

Envoyer des données de télémétrie

Lorsque vous incluez cette fonctionnalité dans la boîte de dialogue de configuration, le programme d'installation définit la variable d'environnement `EC2LAUNCH_TELEMETRY` sur une valeur de 1. Si vous désactivez Envoyer des données de télémétrie, le programme d'installation définit la valeur de la variable d'environnement sur 0.

Lorsque l'agent EC2Launch v2 s'exécute, il lit la variable d'environnement `EC2LAUNCH_TELEMETRY` pour déterminer si les données de télémétrie doivent être chargées. Si la valeur est égale à 1, il charge les données. Dans le cas contraire, il ne les charge pas.

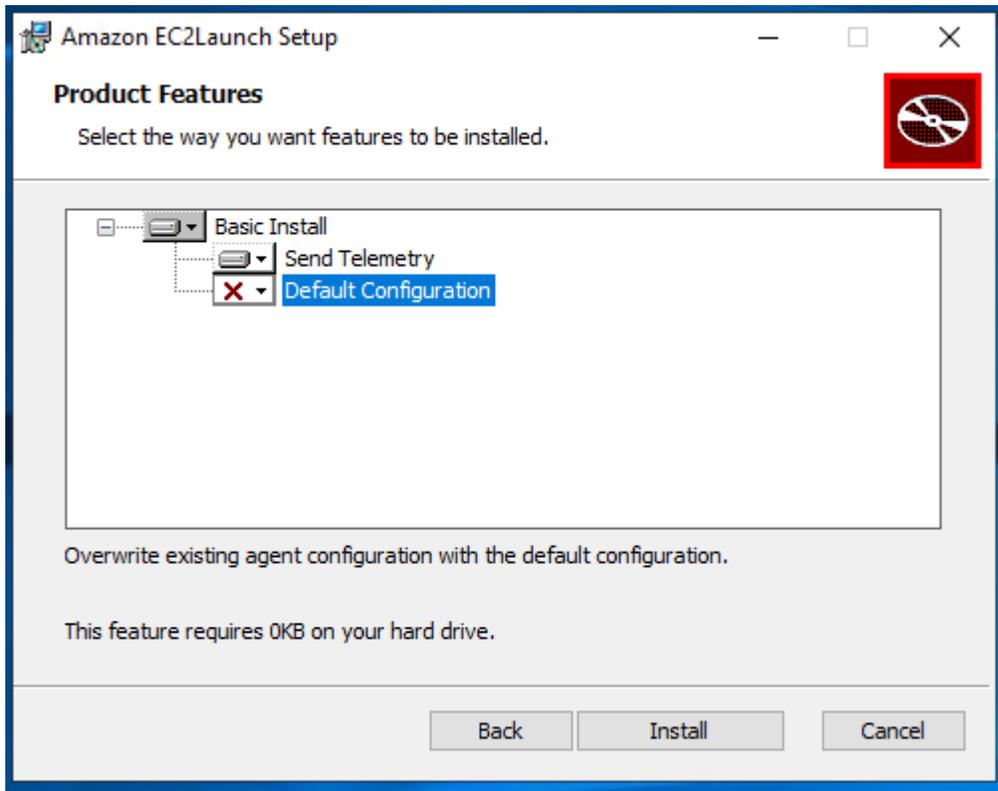
Configuration par défaut

La configuration par défaut pour EC2Launch v2 consiste à remplacer l'agent de lancement local s'il existe déjà. La première fois que vous exécutez une installation sur une instance, la configuration par défaut effectue une installation propre. Si vous désactivez la configuration par défaut lors de l'installation initiale, l'installation échoue.

Si vous réexécutez l'installation sur l'instance, vous pouvez désactiver la configuration par défaut afin d'effectuer une mise à niveau qui ne remplace pas le fichier `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`.

Exemple : mise à niveau d'EC2Launch v2 grâce à la télémétrie

L'exemple suivant montre la boîte de dialogue de configuration d'EC2Launch v2 configurée pour mettre à niveau l'installation actuelle et activer la télémétrie. Cette configuration effectue une installation sans remplacer le fichier de configuration de l'agent et définit la valeur de la variable d'environnement EC2LAUNCH_TELEMETRY sur 1.



Command line

Lorsque vous installez ou mettez à niveau EC2Launch v2, vous pouvez configurer les options d'installation suivantes avec la commande `msiexec` dans un shell de ligne de commande.

Valeurs de paramètres **ADDLOCAL**

De base (obligatoire)

Installez l'agent de lancement. Si cette valeur n'est pas présente dans le paramètre `ADDLOCAL`, l'installation se termine.

Propre

Lorsque vous incluez la valeur `Clean` dans le paramètre `ADDLOCAL`, le programme d'installation écrit le fichier de configuration de l'agent à l'emplacement suivant : `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Si le fichier de configuration de l'agent existe déjà, il le remplace.

Lorsque vous enlevez la valeur `Clean` du paramètre `ADDLOCAL`, le programme d'installation effectue une mise à niveau qui ne remplace pas le fichier de configuration de l'agent.

Télémétrie

Lorsque vous incluez la valeur `Telemetry` dans le paramètre `ADDLOCAL`, le programme d'installation définit la valeur de la variable d'environnement `EC2LAUNCH_TELEMETRY` sur `1`.

Lorsque vous enlevez la valeur `Telemetry` du paramètre `ADDLOCAL`, le programme d'installation définit la valeur de la variable d'environnement sur `0`.

Lorsque l'agent `EC2Launch v2` s'exécute, il lit la variable d'environnement `EC2LAUNCH_TELEMETRY` pour déterminer si les données de télémétrie doivent être chargées. Si la valeur est égale à `1`, il charge les données. Dans le cas contraire, il ne les charge pas.

Exemple : installation d'EC2Launch v2 avec télémétrie

```
& msixec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"  
ADDLOCAL="Basic,Clean,Telemetry" /q
```

Vérification de la version d'EC2Launch v2

Utilisez l'une des procédures suivantes pour vérifier quelle version d'EC2Launch v2 est installée sur vos instances.

Windows PowerShell

Vérifiez la version installée d'EC2Launch v2 avec Windows PowerShell, comme suit.

1. Lancez une instance depuis votre AMI et connectez-vous à celle-ci.
2. Exécutez la commande suivante PowerShell pour vérifier la version installée d'EC2Launch v2 :

```
& "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
```

Windows Control Panel

Vérifiez la version installée d'EC2Launch v2 dans le panneau de configuration Windows, comme suit.

1. Lancez une instance depuis votre AMI et connectez-vous à celle-ci.
2. Ouvrez le panneau de configuration Windows, puis choisissez Programmes et fonctionnalités.
3. Recherchez Amazon EC2Launch dans la liste des programmes installés. Son numéro de version s'affiche dans la colonne Version.

Pour consulter les dernières mises à jour des AMI AWS Windows, consultez [l'historique des versions des AMI Windows](#) dans le Guide de référence des AMI AWS Windows.

Pour obtenir la version la plus récente d'EC2Launch v2, consultez [Historique des versions EC2Launch v2](#).

Pour obtenir la dernière version de l'outil de migration EC2Launch v2, consultez [Historique des versions de l'outil de migration EC2Launch v2](#).

Vous pouvez recevoir des notifications en cas de publication de nouvelles versions du service EC2Launch v2. Pour plus d'informations, consultez [S'abonner aux notifications du service EC2Launch v2](#).

Migrer vers EC2Launch v2

L'outil de migration EC2Launch met à niveau l'agent de lancement installé (EC2Config et EC2Launch v1) en le désinstallant et en installant EC2Launch v2. Les configurations applicables des services de lancement précédents sont automatiquement migrées vers le nouveau service. L'outil de migration ne détecte aucune tâche planifiée liée aux scripts EC2Launch v1 ; par conséquent, il ne définit pas automatiquement ces tâches dans EC2Launch v2. Pour configurer ces tâches, modifiez le fichier [agent-config.yml](#) ou utilisez la [boîte de dialogue des paramètres d'EC2Launch v2](#). Par exemple, si une tâche planifiée sur une instance exécute `InitializeDisks.ps1`, après avoir exécuté l'outil de migration, vous devez spécifier les volumes que vous souhaitez initialiser dans la boîte de dialogue des paramètres d'EC2Launch v2. Voir l'étape 6 de la procédure pour [Modifier les paramètres à l'aide de la boîte de dialogue des paramètres EC2Launch v2](#).

Vous pouvez télécharger l'outil de migration ou l'installer à l'aide d'un RunCommand document SSM.

Vous pouvez télécharger l'outil à partir des emplacements suivants :

Note

Le lien vers l'outil de migration 32 bits sera obsolète. Nous vous recommandons d'utiliser le lien 64 bits pour migrer vers EC2Launch v2. Si vous avez besoin d'un agent de lancement 32 bits, utilisez [EC2Config](#).

- 64 bits — <https://s3.amazonaws.com/amazon-ec2launch-v2-utils/MigrationTool/Windows/amd64/latest/EC2Tool.zip> [LaunchMigration](#)
- 32 bits — <https://s3.amazonaws.com/amazon-ec2launch-v2-utils/MigrationTool/Windows/386/latest/EC2Tool.zip> [LaunchMigration](#)

Note

Vous devez exécuter l'outil de migration EC2Launch v2 en tant qu'administrateur. EC2Launch v2 est installé en tant que service après avoir exécuté l'outil de migration. Il ne s'exécute pas immédiatement. Par défaut, il s'exécute au démarrage de l'instance et si une instance est arrêtée puis démarrée ultérieurement ou redémarrée.

Utilisez le document SSM [AWSEC2Launch-RunMigration](#) pour migrer vers la dernière version d'EC2Launch v2 avec Run Command SSM. Le document ne nécessite aucun paramètre. Pour plus d'informations sur l'utilisation de Run Command SSM, consultez [AWS Systems Manager Run Command](#).

L'outil de migration applique les configurations suivantes d'EC2Config à EC2Launch v2.

- Si `Ec2DynamicBootVolumeSize` est défini sur `false`, supprime l'étape EC2Launch v2 boot
- Si `Ec2SetPassword` est défini sur `Enabled`, définit le type de mot de passe EC2Launch v2 sur `random`
- Si `Ec2SetPassword` est défini sur `Disabled`, définit le type de mot de passe EC2Launch v2 sur `nothing`
- Si `SetDnsSuffixList` est défini sur `false`, supprime la tâche EC2Launch v2 `setDnsSuffix`
- Si `EC2SetComputerName` est défini sur `true`, ajoute la tâche EC2Launch v2 `setHostName` à la configuration `yaml`

L'outil de migration applique les configurations suivantes d'EC2Launch v1 à EC2Launch v2.

- Si `ExtendBootVolumeSize` est défini sur `false`, supprime l'étape EC2Launch v2 boot
- Si `AdminPasswordType` est défini sur `Random`, définit le type de mot de passe EC2Launch v2 sur `random`
- Si `AdminPasswordType` est défini sur `Specify`, définit le type de mot de passe EC2Launch v2 sur `static` et les données de mot de passe sur le mot de passe spécifié dans `AdminPassword`
- Si `SetWallpaper` est défini sur `false`, supprime la tâche EC2Launch v2 `setWallpaper`
- Si `AddDnsSuffixList` est défini sur `false`, supprime la tâche EC2Launch v2 `setDnsSuffix`
- Si `SetComputerName` est défini sur `true`, ajoute la tâche EC2Launch v2 `setHostName`

Arrêter, redémarrer, supprimer ou désinstaller EC2Launch v2

Vous pouvez gérer le service EC2Launch v2 comme vous le feriez pour n'importe quel autre service Windows.

EC2Launch v2 s'exécute une fois au démarrage et exécute toutes les tâches configurées. Après l'exécution des tâches, le service entre dans un état arrêté. Lorsque vous redémarrez le service, le service exécute à nouveau toutes les tâches configurées et revient à un état arrêté.

Pour appliquer les paramètres mis à jour dans votre instance, vous pouvez arrêter et redémarrer le service. Si vous installez manuellement EC2Launch v2, vous devez d'abord arrêter le service.

Pour arrêter le service EC2Launch v2

1. Lancez et connectez-vous à votre instance Windows.
2. Dans le menu Démarrer, choisissez Outils d'administration, puis ouvrez Services.
3. Dans la liste des services, cliquez avec le bouton droit sur Amazon EC2Launch, puis sélectionnez Arrêter.

Pour redémarrer le service EC2Launch v2

1. Lancez et connectez-vous à votre instance Windows.
2. Dans le menu Démarrer, choisissez Outils d'administration, puis ouvrez Services.
3. Dans la liste des services, cliquez avec le bouton droit sur Amazon EC2Launch, puis sélectionnez Redémarrer.

Si vous n'avez pas besoin de mettre à jour les paramètres de configuration, que vous créez votre propre AMI ou que vous utilisez AWS Systems Manager, vous pouvez supprimer et désinstaller le service. La suppression d'un service entraîne celle de sa sous-clé du registre. La désinstallation d'un service entraîne la suppression des fichiers, des sous-clés du registre et de tous les raccourcis vers le service.

Pour supprimer le service EC2Launch v2

1. Démarrez une fenêtre d'invite de commande.
2. Exécutez la commande suivante :

```
sc delete EC2Launch
```

Pour désinstaller EC2Launch v2

1. Lancez et connectez-vous à votre instance Windows.
2. Dans le menu Start (Démarrer), choisissez Control Panel (Panneau de configuration).
3. Ouvrez Programs (Programmes), puis Programs and Features (Programmes et fonctionnalités).
4. Dans la liste des programmes, choisissez Amazon EC2Launch. Pour confirmer que vous choisissez la version v2, veuillez consulter la colonne Version.
5. Choisissez Désinstaller.

S'abonner aux notifications du service EC2Launch v2

Amazon SNS peut vous notifier en cas de publication de nouvelles versions du service EC2Launch v2. Pour vous abonner à ces notifications, utilisez la procédure suivante.

S'abonner aux notifications EC2Launch v2

1. [Connectez-vous à la console Amazon SNS AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région, car les notifications SNS auxquelles vous vous abonnez ont été créées dans cette région.
3. Dans le panneau de navigation, choisissez Abonnements.
4. Choisissez Créer un abonnement.

5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :
 - a. Pour ARN de rubrique, utilisez l'Amazon Resource Name (ARN) suivant : `arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2`.
 - b. Pour Protocole, choisissez E-mail.
 - c. Pour Point de terminaison, entrez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications.
 - d. Choisissez Créer un abonnement.
6. Vous recevrez un e-mail vous demandant de confirmer votre abonnement. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Chaque fois qu'une nouvelle version du service EC2Launch v2 est publiée, nous envoyons des notifications aux abonnés de la rubrique. Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

1. Ouvrez la console Amazon SNS.
2. Dans le panneau de navigation, sélectionnez Abonnements.
3. Sélectionnez l'abonnement, puis sous Actions, sélectionnez Supprimer des abonnements. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Paramètres EC2Launch v2

Cette section contient des informations sur la configuration des paramètres pour EC2Launch v2.

Les sujets suivants sont notamment abordés :

- [Modifier les paramètres à l'aide de la boîte de dialogue des paramètres EC2Launch v2](#)
- [Structure du répertoire EC2Launch v2](#)
- [Configurer EC2Launch v2 avec la CLI](#)
- [Configuration de tâche EC2Launch v2](#)
- [Codes de sortie EC2Launch v2 et redémarrages](#)
- [EC2Launch v2 et Sysprep](#)

Modifier les paramètres à l'aide de la boîte de dialogue des paramètres EC2Launch v2

La procédure suivante décrit la manière d'utiliser le service la boîte de dialogue des paramètres EC2Launch v2 pour activer ou désactiver les paramètres.

Note

Si vous configurez incorrectement les tâches personnalisées dans le fichier `agent-config.yml` et que vous tentez d'ouvrir la boîte de dialogue des paramètres Amazon EC2Launch, vous recevrez une erreur. Pour un exemple de schéma, consultez [Exemple : agent-config.yml](#).

1. Lancez et connectez-vous à votre instance Windows.
2. Dans le menu Démarrer, choisissez Tous les programmes, puis accédez aux paramètres EC2Launch.

Amazon EC2Launch settings ✕

General | DNS suffix | Wallpaper | Volumes

Set computer name

- Set the computer name of the instance
- Set to "ip- <hex private IPv4 address> "
- Use custom name
- Reboot after setting computer name

Extend boot volume

- Extend OS partition to use free space for boot volume

Set administrator account

- Set administrator account
- Administrator username (leave blank for default)
- Administrator password settings
 - Random (retrieve from console)
 - Specify (temporarily stored in configuration file)
 - Do not set

Start SSM service

- Re-enable and start SSM service after Sysprep

Optimize ENA

- Optimize receive side scaling and receive queue depth

Enable SSH

- Enable OpenSSH for later Windows versions

Enable Jumbo Frames

- Enable Jumbo Frames
- Important: Do not enable Jumbo Frames if you are not familiar with them

Prepare for imaging

3. Sur l'onglet Général de la boîte de dialogue Paramètres de lancement EC2, vous pouvez activer ou désactiver les paramètres suivants.

a. Set Computer Name (Définir le nom de l'ordinateur)

Si ce paramètre est activé (il est désactivé par défaut), le nom d'hôte actuel est comparé au nom d'hôte souhaité à chaque démarrage. Si les noms d'hôte ne correspondent pas, le nom d'hôte est réinitialisé et le système redémarre éventuellement pour récupérer le nouveau nom d'hôte. Si un nom d'hôte personnalisé n'est pas spécifié, il est généré à l'aide de l'adresse IPv4 privée au format hexadécimal, par exemple `ip-AC1F4E6`. Pour empêcher que votre nom d'hôte existant ne soit modifié, n'activez pas ce paramètre.

b. Étendre le volume de démarrage

Ce paramètre étend de manière dynamique `Disk 0/Volume 0` pour inclure l'espace non partitionné. Cela peut être utile lorsque l'instance est démarrée à partir d'un volume du périphérique racine doté d'une taille personnalisée.

c. Définir le compte administrateur

Lorsque cette option est activée, vous pouvez définir les attributs de nom d'utilisateur et de mot de passe pour le compte d'administrateur créé sur votre ordinateur local. Si cette fonctionnalité n'est pas activée, un compte d'administrateur n'est pas créé sur le système après Sysprep. Indiquez un mot de passe dans `adminPassword` uniquement si `adminPasswordType` est `Specify`.

Les types de mots de passe sont définis comme suit :

i. Random

EC2Launch génère un mot de passe et le chiffre à l'aide de la clé de l'utilisateur. Le système désactive ce paramètre après le lancement de l'instance afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.

ii. Specify

EC2Launch utilise le mot de passe que vous spécifiez dans `adminPassword`. Si ce mot de passe ne répond pas aux exigences du système, EC2Launch génère un mot de passe aléatoire à la place. Le mot de passe est stocké dans le fichier `agent-config.yml` sous forme de texte clair et est supprimé une fois que le mot de passe est défini par Sysprep. EC2Launch chiffre le mot de passe à l'aide de la clé de l'utilisateur.

iii. Do not set

EC2Launch utilise le mot de passe que vous spécifiez dans le fichier unattend.xml. Si vous ne spécifiez pas de mot de passe dans unattend.xml, le compte d'administrateur est désactivé.

d. Démarrer le service SSM

Lorsque cette option est sélectionnée, le service Systems Manager est activé pour démarrer à la suite de Sysprep. EC2Launch v2 exécute toutes les tâches décrites [précédemment](#), et SSM Agent traite les requêtes des fonctionnalités Systems Manager telles que Run Command et State Manager.

Vous pouvez utiliser la fonctionnalité Run Command pour mettre à niveau les instances existantes et utiliser la dernière version du service EC2Launch v2 et de SSM Agent. Pour plus d'informations, consultez [Update SSM Agent by using Run Command](#) dans le Guide de l'utilisateur AWS Systems Manager.

e. Optimiser ENA

Lorsque cette option est sélectionnée, les paramètres ENA sont configurés pour garantir que les paramètres ENA de dimensionnement côté réception et de profondeur de file d'attente de réception sont optimisés pour AWS. Pour plus d'informations, consultez [Configuration de l'affinité d'UC RSS](#).

f. Activer SSH

Ce paramètre permet à OpenSSH pour les versions ultérieures de Windows d'autoriser l'administration du système à distance.

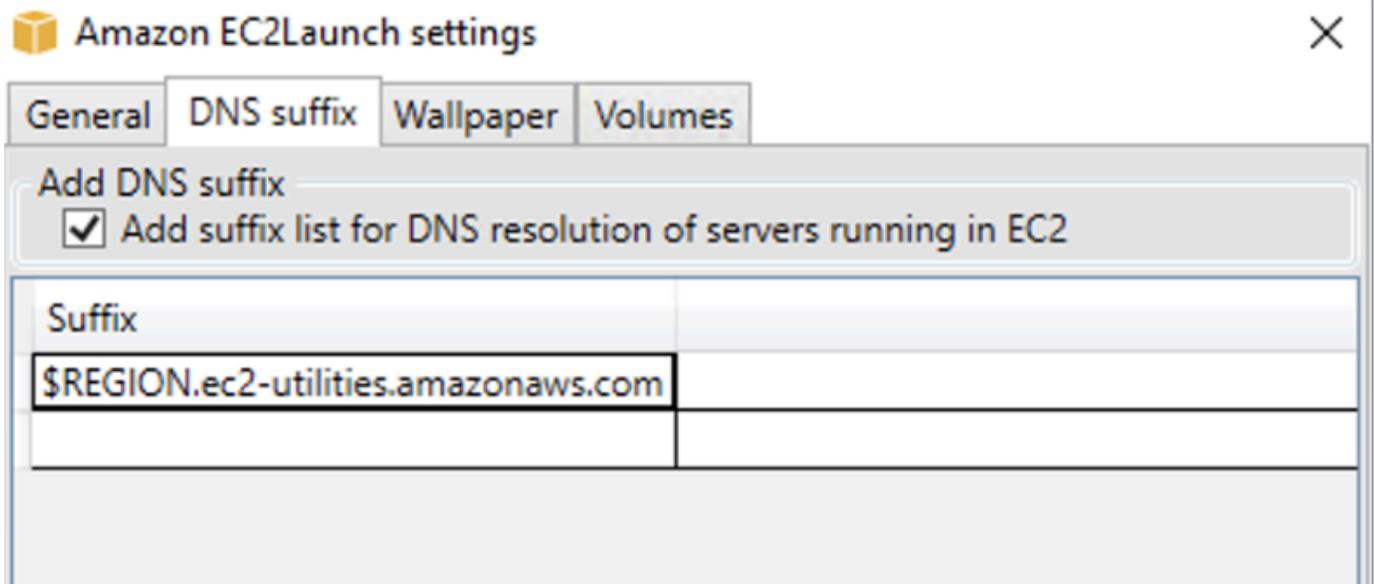
g. Activer les trames Jumbo

Sélectionnez cette option pour activer les trames Jumbo. Les trames Jumbo peuvent avoir des effets inattendus sur vos communications réseau. Assurez-vous donc de comprendre comment les trames Jumbo auront un impact sur votre système avant de les activer. Pour plus d'informations sur les trames jumbo, consultez [Trames jumbo \(MTU de 9001\)](#).

h. Préparer l'imagerie

Indiquez si vous souhaitez que votre instance EC2 s'arrête avec ou sans Sysprep. Lorsque vous souhaitez exécuter Sysprep avec EC2Launch v2, choisissez Arrêter avec Sysprep.

4. Dans l'onglet Suffixe DNS vous pouvez sélectionner si vous souhaitez ajouter une liste de suffixe DNS pour la résolution DNS des serveurs exécutés dans EC2, sans fournir le nom de domaine complet. Les suffixes DNS peuvent contenir les variables \$REGION et \$AZ. Seuls les suffixes qui n'existent pas déjà seront ajoutés à la liste.



5. Dans l'onglet Fond d'écran, vous pouvez configurer le fond d'écran de votre instance avec une image d'arrière-plan et spécifier les détails de l'instance à afficher dans le fond d'écran. Amazon EC2 génère les détails à chaque fois que vous vous connectez.

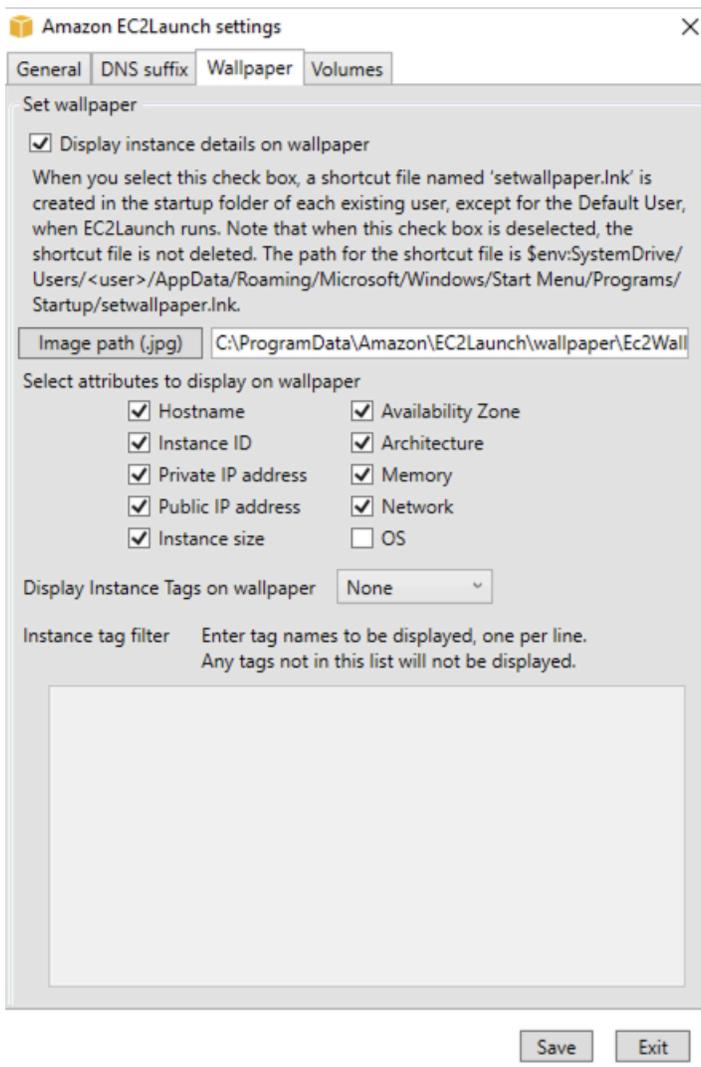
Vous pouvez configurer votre fond d'écran à l'aide des commandes suivantes.

- Afficher les détails de l'instance sur le fond d'écran – Cette case à cocher active ou désactive l'affichage des détails de l'instance sur le fond d'écran.
- Chemin de l'image (.jpg) – Spécifiez le chemin d'accès à l'image à utiliser comme fond d'écran.
- Sélectionner les attributs à afficher sur le fond d'écran – Cochez les cases correspondant aux détails de l'instance que vous voulez voir apparaître sur le fond d'écran. Décochez les cases des détails d'instance précédemment sélectionnés que vous voulez supprimer du fond d'écran.
- Afficher les balises d'instance sur le fond d'écran – Sélectionnez l'un des paramètres suivants pour afficher les balises d'instance sur le fond d'écran :
 - Aucun : n'affiche aucune balise d'instance sur le fond d'écran.
 - Afficher tout : affiche toutes les balises d'instance sur le fond d'écran.

- **Afficher avec filtre** : affiche les balises d'instance spécifiées sur le fond d'écran. Lorsque vous sélectionnez ce paramètre, vous pouvez ajouter les balises d'instance que vous souhaitez voir s'afficher sur votre fond d'écran dans la zone Filtre de balise d'instance.

Note

Vous devez activer les balises dans les métadonnées pour afficher les balises sur le fond d'écran. Pour plus d'informations sur les balises et métadonnées d'instance, consultez [Utiliser les identifications d'instance dans les métadonnées d'instance](#).



6. Sous l'onglet Volumes, indiquez si vous souhaitez initialiser les volumes attachés à l'instance. L'activation définit les lettres de lecteur pour tous les volumes supplémentaires et les étend

pour utiliser l'espace disponible. Si vous sélectionnez Tous, tous les volumes de stockage sont initialisés. Si vous sélectionnez Appareils, seuls les appareils spécifiés dans la liste sont initialisés. Vous devez entrer l'appareil pour chaque appareil à initialiser. Utilisez les appareils répertoriés sur la console EC2, par exemple, xvdb ou /dev/nvme0n1. La liste déroulante affiche les volumes de stockage attachés à l'instance. Pour entrer un appareil qui n'est pas attaché à l'instance, saisissez-le dans le champ de texte.

Nom, Lettre et Partition sont des champs facultatifs. Si aucune valeur n'est spécifiée pour Partition, les volumes de stockage supérieurs à 2 To sont initialisés avec le type de gpt partition, et ceux inférieurs à 2 To sont initialisés avec le type de mbt partition. Si des appareils sont configurés et qu'un appareil non NTFS contient une table de partitions ou que les 4 premiers Ko du disque contiennent des données, le disque est ignoré et l'action est consignée.

Amazon EC2Launch settings ✕

General | DNS suffix | Wallpaper | **Volumes**

Initialize volumes

Initialize All Devices

Devices

If you choose Devices, only the devices listed below are initialized. You must enter the Device for each device to be initialized. Use the devices listed on the EC2 console, for example, xvdb or /dev/nvme0n1. Name, Letter, and Partition are optional.

Device	Name	Letter	Partition
--------	------	--------	-----------

Voici un exemple de fichier YAML de configuration créé à partir des paramètres saisis dans la boîte de dialogue EC2Launch.

```
version: 1.0
config:
  - stage: boot
tasks:
  - task: extendRootPartition
  - stage: preReady
    tasks:
      - task: activateWindows
        inputs:
          activation:
            type: amazon
      - task: setDnsSuffix
        inputs:
          suffixes:
            - $REGION.ec2-utilities.amazonaws.com
      - task: setAdminAccount
        inputs:
          password:
            type: random
      - task: setWallpaper
        inputs:
          path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
          attributes:
            - hostName
            - instanceId
            - privateIpAddress
            - publicIpAddress
            - instanceSize
            - availabilityZone
            - architecture
            - memory
            - network
  - stage: postReady
    tasks:
      - task: startSsm
```

Structure du répertoire EC2Launch v2

EC2Launch v2 doit être installé dans les répertoires suivants :

- Binaires de service : %ProgramFiles%\Amazon\EC2Launch
- Données de service (paramètres, fichiers journaux et fichiers d'état) : %ProgramData%\Amazon\EC2Launch

Note

Par défaut, Windows masque les fichiers et les dossiers qui se trouvent sous C : \ProgramData. Pour afficher les fichiers et les répertoires EC2Launch v2, vous devez entrer le chemin d'accès dans l'explorateur Windows ou modifier les propriétés de dossier afin d'afficher les fichiers et les dossiers cachés.

Le répertoire %ProgramFiles%\Amazon\EC2Launch contient des binaires et des bibliothèques de support. Il comprend les sous-répertoires suivants :

- settings
 - EC2LaunchSettingsUI.exe — Interface utilisateur pour modifier le fichier agent-config.yml
 - Yam1DotNet.dll — DLL pour prendre en charge certaines opérations dans l'interface utilisateur
- tools
 - ebsnvme-id.exe — Outil pour examiner les métadonnées des volumes EBS sur l'instance
 - AWSAcpiSpcrReader.exe — Outil pour déterminer le port COM correct à utiliser
 - EC2LaunchEventMessage.dll — DLL pour prendre en charge la journalisation des événements Windows pour EC2Launch
- service
 - EC2LaunchService.exe — Exécutable de service Windows qui est lancé lorsque l'agent de lancement s'exécute en tant que service.
- EC2Launch.exe — Exécutable principal EC2Launch
- EC2LaunchAgentAttribution.txt — Attribution du code utilisé dans EC2 Launch

Le répertoire %ProgramData%\Amazon\EC2Launch contient les sous-répertoires suivants. Toutes les données produites par le service, y compris les journaux, la configuration et l'état, sont stockées dans ce répertoire.

- `config` — Configuration

Le fichier de configuration du service est stocké dans ce répertoire sous la forme de `agent-config.yml`. Ce fichier peut être mis à jour pour modifier, ajouter ou supprimer des tâches exécutées par le service par défaut. L'autorisation de créer des fichiers dans ce répertoire est limitée au compte administrateur pour empêcher l'escalade des privilèges.

- `log` — Journaux d'instances

Les journaux pour le service (`agent.log`), la console (`console.log`), les performances (`bench.log`) et les erreurs (`error.log`) sont stockés dans ce répertoire. Les fichiers journaux sont ajoutés lors des exécutions ultérieures du service.

- `state` — Données sur l'état du service

L'état utilisé par le service pour déterminer les tâches à exécuter est stocké ici. Il existe un fichier `.run-once` qui indique si le service a déjà été exécuté après Sysprep (donc les tâches avec une fréquence d'une fois seront ignorées lors de la prochaine exécution). Ce sous-répertoire inclut un `state.json` et `previous-state.json` pour suivre l'état de chaque tâche.

- `sysprep` — Sysprep

Ce répertoire contient des fichiers qui sont utilisés pour déterminer les opérations à effectuer par Sysprep lorsqu'il crée une AMI Windows personnalisée qui peut être réutilisée.

Configurer EC2Launch v2 avec la CLI

Vous pouvez utiliser la CLI (CLI) pour configurer vos paramètres EC2Launch et gérer le service. La section suivante contient des descriptions et des informations d'utilisation des commandes CLI que vous pouvez utiliser pour gérer EC2Launch v2.

Commandes

- [collect-logs](#)
- [get-agent-config](#)
- [list-volumes](#)
- [reset](#)
- [run](#)
- [status](#)
- [sysprep](#)

- [valider](#)
- [version](#)
- [fond d'écran](#)

collect-logs

Collecte les fichiers journaux pour EC2Launch, compile les fichiers et les place dans un répertoire spécifié.

Exemple

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Utilisation

```
ec2launch collect-logs [flags]
```

Indicateurs

-h, --help

aide pour collect-logs

-o, --output string

chemin d'accès aux fichiers journaux de sortie compressés

get-agent-config

Imprime agent-config.yml au format spécifié (JSON ou YAML). Si aucun format n'est spécifié, agent-config.yml est imprimé dans le format précédemment spécifié.

Exemple

```
ec2launch get-agent-config -f json
```

Exemple 2

Les PowerShell commandes suivantes indiquent comment modifier et enregistrer le agent-config fichier au format JSON.

```
$config = & "$env:ProgramFiles/Amazon/EC2Launch/EC2Launch.exe" --format json |
  ConvertFrom-Json
$jumboFrame =@"
{
  "task": "enableJumboFrames"
}
"@
$config.config | %{if($_.stage -eq 'postReady'){$_tasks += (ConvertFrom-Json -
InputObject $jumboFrame)}}
$config | ConvertTo-Json -Depth 6 | Out-File -encoding UTF8
$env:ProgramData/Amazon/EC2Launch/config/agent-config.yml
```

Utilisation

```
ec2launch get-agent-config [flags]
```

Indicateurs

-h, --help

aide pour get-agent-config

-f, --format string

format de sortie du fichier agent-config : json, yaml

list-volumes

Répertorie tous les volumes de stockage attachés à l'instance, y compris les volumes éphémères et EBS.

Exemple

```
ec2launch list-volumes
```

Utilisation

```
ec2launch list-volumes
```

Indicateurs

-h, --help

aide pour `list-volumes`

reset

L'objectif principal de cette tâche est de réinitialiser l'agent pour sa prochaine exécution. Pour ce faire, la commande `reset` supprime toutes les données d'état de l'agent pour EC2Launch v2 du répertoire EC2Launch local (consultez [Structure du répertoire EC2Launch v2](#)). `Reset` supprime éventuellement le service et les journaux Sysprep.

Le comportement des scripts dépend du mode dans lequel l'agent exécute les scripts : en ligne ou détaché.

En ligne (par défaut)

L'agent EC2Launch v2 exécute les scripts un par un (`detach: false`). Il s'agit du paramètre par défaut.

Note

Lorsque votre script en ligne émet une commande `reset` ou `sysprep`, il s'exécute immédiatement et réinitialise l'agent. La tâche en cours se termine, puis l'agent s'arrête sans exécuter d'autres tâches.

Par exemple, si la tâche qui émet la commande aurait été suivie d'une tâche `startSsm` (incluse par défaut après l'exécution des données utilisateur), la tâche ne s'exécute pas et le service Systems Manager ne démarre jamais.

Detached

L'agent EC2Launch v2 exécute des scripts simultanément avec d'autres tâches (`detach: true`).

Note

Lorsque votre script détaché émet une commande `reset` ou `sysprep`, ces commandes attendent que l'agent ait terminé leur exécution avant de s'exécuter. Les tâches exécutées après `executeScript` se poursuivront.

Exemple

```
ec2launch reset -c
```

Utilisation

```
ec2launch reset [flags]
```

Indicateurs

-c, --clean

nettoie les journaux d'instance avant la reset

-h, --help

aide pour reset

run

Exécutions d'EC2Launch v2.

Exemple

```
ec2launch run
```

Utilisation

```
ec2launch run [flags]
```

Indicateurs

-h, --help

aide pour run

status

Obtient le statut de l'agent EC2Launch v2. Il est possible de bloquer le processus jusqu'à ce que l'agent soit terminé. Le code de sortie du processus détermine l'état de l'agent :

- 0 : l'agent a été exécuté avec succès.

- 1 : l'agent a été exécuté et a échoué.
- 2 : l'agent est toujours en cours d'exécution.
- 3 : l'agent est dans un état inconnu. L'état de l'agent n'est pas en cours d'exécution ou arrêté.
- 4 : une erreur s'est produite lors de la tentative de récupération de l'état de l'agent.
- 5 : l'agent n'est pas en cours d'exécution et l'état de la dernière exécution connue est inconnu. Cela peut signifier :
 - qu'à la fois `state.json` et `previous-state.json` sont supprimés.
 - que `previous-state.json` est corrompu.

Il s'agit de l'état de l'agent après l'exécution de la commande [reset](#).

Exemple :

```
ec2launch status -b
```

Utilisation

```
ec2launch status [flags]
```

Indicateurs

`-b, --block`

bloque le processus jusqu'à la fin de l'exécution de l'agent

`-h, --help`

aide pour status

sysprep

L'objectif principal de cette tâche est de réinitialiser l'agent pour sa prochaine exécution. Pour ce faire, la commande `sysprep` réinitialise l'état de l'agent, met à jour le fichier `unattend.xml`, désactive RDP et exécute Sysprep.

Le comportement des scripts dépend du mode dans lequel l'agent exécute les scripts : en ligne ou détaché.

En ligne (par défaut)

L'agent EC2Launch v2 exécute les scripts un par un (`detach: false`). Il s'agit du paramètre par défaut.

Note

Lorsque votre script en ligne émet une commande `reset` ou `sysprep`, il s'exécute immédiatement et réinitialise l'agent. La tâche en cours se termine, puis l'agent s'arrête sans exécuter d'autres tâches.

Par exemple, si la tâche qui émet la commande aurait été suivie d'une tâche `startSsm` (incluse par défaut après l'exécution des données utilisateur), la tâche ne s'exécute pas et le service Systems Manager ne démarre jamais.

Detached

L'agent EC2Launch v2 exécute des scripts simultanément avec d'autres tâches (`detach: true`).

Note

Lorsque votre script détaché émet une commande `reset` ou `sysprep`, ces commandes attendent que l'agent ait terminé leur exécution avant de s'exécuter. Les tâches exécutées après `executeScript` se poursuivront.

Exemple :

```
ec2launch sysprep
```

Utilisation

```
ec2launch sysprep [flags]
```

Indicateurs

```
-c,--clean
```

nettoie les journaux d'instance avant la sysprep

`-h, --help`

aide pour Sysprep

`-s, --shutdown`

arrête l'instance après l'exécution de sysprep

valider

Valide le fichier agent-config C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml.

Exemple

```
ec2launch validate
```

Utilisation

```
ec2launch validate [flags]
```

Indicateurs

`-h, --help`

aide pour validate

version

Obtient la version exécutable.

Exemple

```
ec2launch version
```

Utilisation

```
ec2launch version [flags]
```

Indicateurs

-h, --help

aide pour version

fond d'écran

Définit le nouveau fond d'écran sur le chemin d'écran fourni (fichier .jpg) et affiche les détails de l'instance sélectionnée.

Syntaxe

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,instanceSize,availabilityZone, a
```

Inputs

Paramètres

--allowed-tags [***tag-name-1, tag-name-n***]

(Facultatif) Tableau JSON codé en Base64 contenant les noms des balises d'instance à afficher sur le fond d'écran. Vous pouvez utiliser cette balise ou l'option `--all-tags`, mais pas les deux.

--attributes ***attribute-string-1, attribute-string-n***

(Facultatif) Une liste de chaînes d'attributs `wallpaper` séparées par des virgules pour appliquer des paramètres au fond d'écran.

[--path | -p] ***path-string***

(Obligatoire) Spécifie le chemin du fichier image d'arrière-plan `wallpaper`.

Indicateurs

--all-tags

(Facultatif) Affiche toutes les balises d'instance sur le fond d'écran. Vous pouvez utiliser cette balise ou l'option `--allowed-tags`, mais pas les deux.

`--help | -h`

Affiche l'aide concernant la commande wallpaper.

Configuration de tâche EC2Launch v2

Cette section inclut les schémas de configuration, les tâches, les détails et les exemples pour `agent-config.yml` et les données utilisateur.

Tâches et exemples

- [Schéma : agent-config.yml](#)
- [Schéma : données utilisateur](#)
- [Définitions de tâche](#)

Schéma : **agent-config.yml**

La structure du fichier `agent-config.yml` est illustrée ci-dessous. Notez qu'une tâche ne peut pas être répétée dans la même étape. Pour connaître les propriétés des tâches, consultez les descriptions de tâches suivantes.

Structure du document : `agent-config.yml`

JSON

```
{
  "version": "1.0",
  "config": [
    {
      "stage": "string",
      "tasks": [
        {
          "task": "string",
          "inputs": {
            ...
          }
        },
        ...
      ]
    },
    ...
  ]
}
```

```
}
```

YAML

```
version: 1.0
config:
- stage: string
  tasks:
  - task: string
inputs:
  ...
  ...
  ...
```

Exemple : **agent-config.yml**

L'exemple suivant montre les paramètres du fichier de configuration `agent-config.yml`.

```
version: 1.0
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
```

```
- privateIpAddress
- publicIpAddress
- instanceSize
- availabilityZone
- architecture
- memory
- network
- stage: postReady
  tasks:
  - task: startSsm
```

Schéma : données utilisateur

Les exemples JSON et YAML suivants illustrent la structure du document pour les données utilisateur. Amazon EC2 analyse chaque tâche nommée du tableau `tasks` que vous spécifiez dans le document. Chaque tâche possède son propre ensemble de propriétés et d'exigences. Pour obtenir des détails, veuillez consulter le [Définitions de tâche](#).

Note

Une tâche ne doit apparaître qu'une seule fois dans le tableau des tâches de données utilisateur.

Structure du document : données utilisateur

JSON

```
{
  "version": "1.1",
  "tasks": [
    {
      "task": "string",
      "inputs": {
        ...
      },
    },
    ...
  ]
}
```

YAML

```
version: 1.1
tasks:
- task: string
  inputs:
    ...
  ...
```

Exemple : données utilisateur

Pour plus d'informations sur les rôles d'utilisateur, consultez [Comment Amazon EC2 gère les données utilisateur pour les instances Windows](#).

L'exemple de document YAML suivant montre un PowerShell script qu'EC2Launch v2 exécute sous forme de données utilisateur pour créer un fichier.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

Vous pouvez utiliser un format XML pour les données utilisateur compatible avec les versions précédentes de l'agent de lancement. EC2Launch v2 exécute le script en tant que tâche `executeScript` dans l'étape `UserData`. Pour se conformer au comportement d'EC2Launch v1 et d'EC2Config, le script de données utilisateur s'exécute par défaut en tant que processus attaché/en ligne.

Vous pouvez ajouter des balises facultatives pour personnaliser l'exécution de votre script. Par exemple, pour exécuter le script de données utilisateur lors du redémarrage de l'instance et lors du lancement de l'instance, vous pouvez utiliser la balise suivante :

```
<persist>true</persist>
```

Exemple :

```
<powershell>
```

```
$file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Vous pouvez spécifier un ou plusieurs PowerShell arguments à l'aide de la `<powershellArguments>` balise. Si aucun argument n'est transmis, EC2Launch v2 ajoute l'argument suivant par défaut : `-ExecutionPolicy Unrestricted`

Exemple :

```
<powershell>
$file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Pour exécuter un script de données utilisateur XML en tant que processus détaché, ajoutez la balise suivante à vos données utilisateur.

```
<detach>true</detach>
```

Exemple :

```
<powershell>
$file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

Note

La balise `detach` n'est pas prise en charge sur les agents de lancement précédents.

Journal des modifications : données utilisateur

Le tableau suivant répertorie les modifications apportées aux données utilisateur et les recoupe à la version de l'agent EC2Launch v2 qui s'applique.

Version des données utilisateur	Détails	Présenté dans
1.1	<ul style="list-style-type: none"> • Les tâches relatives aux données utilisateur s'exécutent avant l'étape PostReady dans le fichier de configuration de l'agent. • Exécute les données utilisateur avant de démarrer l'agent Systems Manager (même comportement que EC2Launch v1 et EC2Config).* 	EC2Launch v2 version 2.0.1245
1.0	<ul style="list-style-type: none"> • Deviendra obsolète. • Les tâches relatives aux données utilisateur s'exécutent après l'étape PostReady dans le fichier de configuration de l'agent. Ce n'est pas rétrocompatible avec EC2Launch v1. • Affecté par une condition de concurrence entre les tâches de démarrage et de données utilisateur de l'agent Systems Manager. 	EC2Launch v2 version 2.0.0

* Lorsqu'il est utilisé avec le fichier `agent-config.yml` par défaut.

Définitions de tâche

Chaque tâche possède son propre ensemble de propriétés et d'exigences. Pour plus de détails, consultez les tâches individuelles à inclure dans votre document.

Tâches

- [activateWindows](#)
- [enableJumboFrames](#)
- [enableOpenSsh](#)
- [executeProgram](#)
- [executeScript](#)

- [extendRootPartition](#)
- [initializeVolume](#)
- [optimizeEna](#)
- [ensemble AdminAccount](#)
- [setDnsSuffix](#)
- [setHostName](#)
- [setWallpaper](#)
- [startSsm](#)
- [sysprep](#)
- [writeFile](#)

activateWindows

Active Windows sur un ensemble de AWS KMS serveurs. L'activation est ignorée si l'instance est détectée comme étant de type Apportez votre propre licence (BYOL).

Fréquence — Une fois

AllowedStages — [PreReady]

Entrées —

activation : (carte)

type : type d'activation (string) à utiliser, défini sur amazon

Exemple

```
task: activateWindows
inputs:
  activation:
    type: amazon
```

enableJumboFrames

Active les trames Jumbo, qui augmentent l'unité de transmission maximale (MTU) de la carte réseau. Pour plus d'informations, consultez [Trames jumbo \(MTU de 9001\)](#).

Fréquence — Toujours

AllowedStages — [PostReady, UserData]

Entrées — Aucune

Exemple

```
task: enableJumboFrames
```

enableOpenSsh

Active Windows OpenSSH et ajoute la clé publique de l'instance au dossier des clés autorisées.

Fréquence — Une fois

AllowedStages — [PreReady, UserData]

Entrées — Aucune

Exemple

L'exemple suivant montre comment activer OpenSSH sur une instance et ajouter la clé publique de l'instance au dossier des clés autorisées. Cette configuration fonctionne uniquement sur les instances exécutant Windows Server 2019 et versions ultérieures.

```
task: enableOpenSsh
```

executeProgram

Exécute un programme avec des arguments facultatifs et une fréquence spécifiée.

Étapes : vous pouvez exécuter la tâche `executeProgram` pendant les étapes `PreReady`, `PostReady` et `UserData`.

Fréquence : configurable, voir Entrées.

Inputs

Vous pouvez configurer les paramètres d'exécution comme suit :

fréquence (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- `once`
- `always`

chemin (chaîne)

(Obligatoire) Le chemin d'accès au fichier de l'exécutable à exécuter.

arguments (liste de chaînes)

(Facultatif) Liste d'arguments séparés par des virgules à fournir au programme en entrée.

runAs (chaîne)

(Obligatoire) Doit être défini sur `localSystem`

Sortie

Toutes les tâches écrivent des entrées du fichier journal dans le fichier `agent.log`. Les résultats supplémentaires de la tâche `executeProgram` sont stockés séparément dans un dossier nommé dynamiquement, comme suit :

```
%LocalAppData%\Temp\EC2Launch#####\outputfilename.tmp
```

Le chemin exact vers les fichiers de sortie est inclus dans le fichier `agent.log`, par exemple :

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Fichiers de sortie pour la tâche `executeProgram`

`ExecuteProgramInputs.tmp`

Contient le chemin de l'exécutable et tous les paramètres d'entrée que la tâche `executeProgram` lui transmet lors de son exécution.

Output.tmp

Contient la sortie d'exécution du programme exécuté par la tâche `executeProgram`.

Err.tmp

Contient les messages d'erreur d'exécution du programme exécuté par la tâche `executeProgram`.

Exemples

Les exemples suivants montrent comment exécuter un fichier exécutable à partir d'un répertoire local sur une instance avec la tâche `executeProgram`.

Exemple 1 : configuration d'un exécutable avec un seul argument

Cet exemple montre une tâche `executeProgram` qui exécute un exécutable d'installation en mode silencieux.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\Users\Administrator\Desktop\setup.exe
  arguments: ['-quiet']
```

Exemple 2 : exécutable VLC avec deux arguments

Cet exemple montre une tâche `executeProgram` qui exécute un fichier exécutable VLC avec deux arguments transmis en tant que paramètres d'entrée.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\vlc-3.0.11-win64.exe
  arguments: ['/L=1033', '/S']
runAs: localSystem
```

executeScript

Exécute un script avec des arguments facultatifs et une fréquence spécifiée. Le comportement des scripts dépend du mode dans lequel l'agent exécute les scripts : en ligne ou détaché.

En ligne (par défaut)

L'agent EC2Launch v2 exécute les scripts un par un (`detach: false`). Il s'agit du paramètre par défaut.

Note

Lorsque votre script en ligne émet une commande `reset` ou `sysprep`, il s'exécute immédiatement et réinitialise l'agent. La tâche en cours se termine, puis l'agent s'arrête sans exécuter d'autres tâches.

Par exemple, si la tâche qui émet la commande aurait été suivie d'une tâche `startSsm` (incluse par défaut après l'exécution des données utilisateur), la tâche ne s'exécute pas et le service Systems Manager ne démarre jamais.

Detached

L'agent EC2Launch v2 exécute des scripts simultanément avec d'autres tâches (`detach: true`).

Note

Lorsque votre script détaché émet une commande `reset` ou `sysprep`, ces commandes attendent que l'agent ait terminé leur exécution avant de s'exécuter. Les tâches exécutées après `executeScript` se poursuivront.

Étapes : vous pouvez exécuter la tâche `executeScript` pendant les étapes `PreReady`, `PostReady` et `UserData`.

Fréquence : configurable, voir Entrées.

Inputs

Vous pouvez configurer les paramètres d'exécution comme suit :

fréquence (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- `once`

- `always`

type (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- `batch`
- `powershell`

arguments (liste de chaînes)

(Facultatif) Une liste d'arguments de chaîne à passer au shell. Ce paramètre n'est pas pris en charge pour type: `batch`. Si aucun argument n'est transmis, EC2Launch v2 ajoute l'argument suivant par défaut : `-ExecutionPolicy Unrestricted`

contenu (chaîne)

(Obligatoire) Contenu du script.

runAs (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- `admin`
- `localSystem`

detach (booléen)

(Facultatif) L'agent EC2Launch v2 exécute par défaut les scripts un par un (`detach: false`). Pour exécuter le script en même temps que d'autres tâches, définissez la valeur sur `true` (`detach: true`).

Note

Codes de sortie de script (y compris `3010`) n'ont aucun effet lorsque `detach` a la valeur `true`.

Sortie

Toutes les tâches écrivent des entrées du fichier journal dans le fichier `agent.log`. Les résultats supplémentaires du script exécuté par la tâche `executeScript` sont stockés séparément dans un dossier nommé dynamiquement, comme suit :

`%LocalAppData%\Temp\EC2Launch#####\outputfilename.ext`

Le chemin exact vers les fichiers de sortie est inclus dans le fichier agent .log, par exemple :

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Fichiers de sortie pour la tâche **executeScript**

UserScript.ext

Contient le script exécuté par la tâche `executeScript`. L'extension de fichier dépend du type de script que vous avez spécifié dans le paramètre `type` de la tâche `executeScript`, comme suit :

- Si le type est `batch`, l'extension du fichier est `.bat`.
- Si le type est `powershell`, l'extension du fichier est `.ps1`.

Output.tmp

Contient la sortie d'exécution du script exécuté par la tâche `executeScript`.

Err.tmp

Contient les messages d'erreur d'exécution du script exécuté par la tâche `executeScript`.

Exemples

Les exemples suivants montrent comment exécuter un script en ligne avec la tâche `executeScript`.

Exemple 1 : fichier texte de sortie Hello World

Cet exemple montre une `executeScript` tâche qui exécute un PowerShell script pour créer un fichier texte « Hello world » sur le C: lecteur.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: admin
  content: |-
```

```
New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Exemple 2 : exécuter deux scripts

Cet exemple montre que la tâche `executeScript` peut exécuter plusieurs scripts et que le type de script ne doit pas nécessairement correspondre.

Le premier script (type: `powershell`) écrit un résumé des processus en cours d'exécution sur l'instance dans un fichier texte situé sur le lecteur C:.

Le second script (type: `batch`) écrit les informations système dans le fichier `Output.tmp`.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  content: |
    Get-Process | Out-File -FilePath C:\Process.txt
  runAs: localSystem
- frequency: always
  type: batch
  content: |
    systeminfo
```

Exemple 3 : configuration d'un système idempotent avec redémarrages

Cet exemple montre une tâche `executeScript` qui exécute un script idempotent pour effectuer la configuration système suivante avec un redémarrage entre chaque étape :

- Renommer l'ordinateur.
- Joindre l'ordinateur au domaine.
- Activer Telnet.

Le script garantit que chaque opération ne s'exécute qu'une seule fois. Cela empêche une boucle de redémarrage et rend le script idempotent.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: localSystem
```

```
content: |-
$name = $env:ComputerName
if ($name -ne $desiredName) {
    Rename-Computer -NewName $desiredName
    exit 3010
}
$domain = Get-ADDomain
if ($domain -ne $desiredDomain)
{
    Add-Computer -DomainName $desiredDomain
    exit 3010
}
$telnet = Get-WindowsFeature -Name Telnet-Client
if (-not $telnet.Installed)
{
    Install-WindowsFeature -Name "Telnet-Client"
    exit 3010
}
```

extendRootPartition

Étend le volume racine pour utiliser tout l'espace disponible sur le disque.

Fréquence — Une fois

AllowedStages — [Boot]

Entrées — Aucune

Exemple

```
task: extendRootPartition
```

initializeVolume

Initialise les volumes vides attachés à l'instance afin qu'ils soient activés et partitionnés. L'agent de lancement ignore l'initialisation s'il détecte que le volume n'est pas vide. Un volume est considéré comme vide si les 4 premiers Kio d'un volume sont vides ou si un volume n'a pas de [disposition de lecteur reconnaissable par Windows](#).

Le paramètre d'entrée `Letter` est toujours appliqué lors de l'exécution de cette tâche, que le lecteur soit déjà initialisé ou non.

La tâche `initializeVolume` effectue ensuite les actions suivantes.

- Définissez les attributs de disque `offline` et `readonly` sur `False`.
- Créez une partition. Si aucun type de partition n'est spécifié dans le paramètre d'entrée `partition`, les valeurs par défaut suivantes s'appliquent :
 - Si la taille de disque est inférieure à 2 To, définissez le type de partition sur `mbr`.
 - Si la taille de disque est supérieure ou égale à 2 To, définissez le type de partition sur `gpt`.
- Formatez le volume au format NTFS.
- Définissez l'étiquette du volume comme suit :
 - Utilisez la valeur du paramètre d'entrée `name`, le cas échéant.
 - Si le volume est éphémère et qu'aucun nom n'a été spécifié, définissez l'étiquette du volume sur `Temporary Storage Z`.
- Si le volume est éphémère (SSD ou HDD, pas Amazon EBS), créez un fichier `Important.txt` à la racine du volume avec le contenu suivant :

```
This is an 'Instance Store' disk and is provided at no additional charge.
```

```
*This disk offers increased performance since it is local to the host
```

```
*The number of Instance Store disks available to an instance vary by instance type
```

```
*DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
```

```
PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY
```

```
For more information, please refer to: Stockage d'instances Amazon EC2.
```

- Réglez la lettre de lecteur sur la valeur spécifiée dans le paramètre d'entrée `letter`.

Étapes : vous pouvez exécuter la tâche `initializeVolume` pendant les étapes `PostReady` et `UserData`.

Fréquence : toujours.

Inputs

Vous pouvez configurer les paramètres d'exécution comme suit :

appareils (liste de cartes)

(Condition) Configuration pour chaque appareil initialisé par l'agent de lancement. Ceci est obligatoire si le paramètre d'entrée `initialize` est défini sur `devices`.

- **appareil** (chaîne, obligatoire) : identifie l'appareil lors de la création de l'instance. Par exemple, xvdb, xvdf ou \dev\nvme0n1.
- **lettre** (chaîne, facultatif) : un caractère. La lettre de lecteur à attribuer.
- **nom** (chaîne, facultatif) : le nom de volume à attribuer.
- **partition** (chaîne, facultatif) : spécifiez l'une des valeurs suivantes pour le type de partition à créer, ou laissez l'agent de lancement par défaut en fonction de la taille du volume :
 - mbr
 - tpt

initialiser (chaîne)

(Obligatoire) Spécifiez exactement l'une des valeurs suivantes :

- all
- devices

Exemples

Voici des exemples de configurations d'entrée pour la tâche `initializeVolume`.

Exemple 1 : Initialiser deux volumes sur une instance

Cet exemple montre une tâche `initializeVolume` qui initialise deux volumes secondaires sur une instance. L'appareil nommé `DataVolume2` dans l'exemple est éphémère.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
    - device: xvdb
      name: DataVolume1
      letter: D
      partition: mbr
    - device: /dev/nvme0n1
      name: DataVolume2
      letter: E
      partition: gpt
```

Exemple 2 : Initialiser des volumes EBS attachés à une instance

Cet exemple montre une tâche `initializeVolume` qui initialise tous les volumes EBS vides qui sont attachés à l'instance.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Optimise les paramètres ENA en fonction du type d'instance actuel ; peut redémarrer l'instance.

Fréquence — Toujours

AllowedStages — [PostReady, UserData]

Entrées — Aucune

Exemple

```
task: optimizeEna
```

ensemble AdminAccount

Définit les attributs du compte d'administrateur par défaut créé sur la machine locale.

Fréquence — Une fois

AllowedStages — [PreReady]

Entrées —

`name` : nom (chaîne) du compte administrateur

`password` : (carte)

`type` : stratégie (chaîne) pour définir le mot de passe, comme `static`, `random` ou `doNothing`

`data` : (chaîne) stocke les données si le champ `type` est statique

Exemple

```
task: setAdminAccount
inputs:
```

```
name: Administrator
password:
  type: random
```

setDnsSuffix

Ajoute les suffixes DNS à la liste des suffixes de recherche. Seuls les suffixes qui n'existent pas déjà sont ajoutés à la liste. Pour plus d'informations sur la façon dont les agents de lancement définissent les suffixes DNS, consultez. [Configurer le suffixe DNS pour les agents de lancement Windows](#)

Fréquence — Toujours

AllowedStages — [PreReady]

Entrées —

suffixes : (liste de chaînes) liste d'un ou plusieurs suffixes DNS valides ; les variables de substitution valides sont \$REGION et \$AZ

Exemple

```
task: setDnsSuffix
inputs:
  suffixes:
    - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Définit le nom d'hôte de l'ordinateur sur une chaîne personnalisée ou, si `hostName` n'est pas spécifié, l'adresse IPv4 privée.

Fréquence — Toujours

AllowedStages — [PostReady, UserData]

Entrées —

hostName : (chaîne) nom d'hôte facultatif, qui doit être formaté comme suit.

- Doit contenir 15 caractères ou moins
- Doit contenir uniquement des caractères alphanumériques (a-z, A-Z, 0-9) et tiret (-).
- Ne doit pas être entièrement composé de caractères numériques.

`reboot` : (booléen) indique si un redémarrage est autorisé lorsque le nom d'hôte est modifié

Exemple

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Crée le fichier de raccourci `setwallpaper.lnk` dans le dossier de démarrage de chaque utilisateur existant, sauf pour `Default User`. Ce fichier de raccourci s'exécute lorsque l'utilisateur se connecte pour la première fois après le démarrage de l'instance. Il configure l'instance avec un fond d'écran personnalisé qui affiche les attributs de l'instance.

Le chemin du fichier de raccourci est le suivant :

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk
```

Note

Lorsque vous supprimez la tâche `setWallpaper`, ce fichier de raccourci n'est pas supprimé. Pour plus d'informations, consultez [La tâche setWallpaper n'est pas activée, mais le fond d'écran se réinitialise au redémarrage.](#)

Étapes : vous pouvez configurer le fond d'écran au cours des étapes `PreReady` et `UserData`.

Fréquence : `always`

Configuration du fond d'écran

Vous pouvez utiliser les paramètres suivants pour configurer votre fond d'écran.

Inputs

Paramètres d'entrée que vous fournissez et attributs que vous pouvez définir pour configurer votre fond d'écran :

attributs (liste de chaînes)

(Facultatif) Vous pouvez ajouter un ou plusieurs des attributs suivants à votre fond d'écran :

- `architecture`
- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`
- `memory`
- `network`
- `privateIpAddress`
- `publicIpAddress`

instanceTags

(Facultatif) Vous pouvez utiliser exactement l'une des options suivantes pour ce paramètre.

- `AllTags(string)` — Ajoutez toutes les balises d'instance à votre fond d'écran.

```
instanceTags: AllTags
```

- `instanceTags (liste de chaînes)` – Spécifiez une liste de noms de balises d'instance à ajouter à votre fond d'écran. Par exemple :

```
instanceTags:  
  - Tag 1  
  - Tag 2
```

chemin (chaîne)

(Obligatoire) Le chemin du nom du fichier image au format `.jpg` local à utiliser pour votre image de fond d'écran.

Exemple

L'exemple suivant montre les entrées de configuration du fond d'écran qui définissent le chemin du fichier pour l'image d'arrière-plan du fond d'écran, ainsi que les balises d'instance nommées `Tag 1` et `Tag 2`, ainsi que les attributs qui incluent le nom d'hôte, l'ID d'instance et les adresses IP privées et publiques de l'instance.

```
task: setWallpaper
inputs:
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
    - hostName
    - instanceId
    - privateIpAddress
    - publicIpAddress
  instanceTags:
    - Tag 1
    - Tag 2
```

Note

Vous devez activer les balises dans les métadonnées pour afficher les balises sur le fond d'écran. Pour plus d'informations sur les balises et métadonnées d'instance, consultez [Utiliser les identifications d'instance dans les métadonnées d'instance](#).

startSsm

Démarrez le service Systems Manager (SSM) après Sysprep.

Fréquence — Toujours

AllowedStages — [PostReady, UserData]

Entrées — Aucune

Exemple

```
task: startSsm
```

sysprep

Réinitialise l'état du service, met à jour unattend.xml, désactive RDP et exécute Sysprep. Cette tâche s'exécute uniquement une fois que toutes les autres tâches sont terminées.

Fréquence — Une fois

AllowedStages — [UserData]

Entrées —

`clean` : (booléen) nettoie les journaux d'instance avant d'exécuter Sysprep

`shutdown` : (booléen) arrête l'instance après avoir exécuté Sysprep

Exemple

```
task: sysprep
inputs:
  clean: true
  shutdown: true
```

writeFile

Écrit un fichier vers une destination.

Fréquence — voir Entrées

AllowedStages — [PostReady, UserData]

Entrées —

`frequency` : (chaîne) `once` ou `always`

`destination` : (chaîne) chemin vers lequel écrire le contenu

`content` : (chaîne) texte à écrire dans la destination

Exemple

```
task: writeFile
inputs:
- frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Codes de sortie EC2Launch v2 et redémarrages

Vous pouvez utiliser EC2Launch v2 pour définir la manière dont les codes de sortie sont gérés par vos scripts. Par défaut, le code de sortie de la dernière commande exécutée dans un script est signalé comme le code de sortie pour l'ensemble du script. Par exemple, si un script inclut trois commandes et que la première commande échoue mais que les suivantes réussissent, le statut d'exécution est signalé comme `success` étant donné que la commande finale a réussi.

Si vous souhaitez qu'un script redémarre une instance, vous devez spécifier `exit 3010` dans votre script, même lorsque le redémarrage est la dernière étape de votre script. `exit 3010` indique à EC2Launch v2 de redémarrer l'instance et d'appeler à nouveau le script jusqu'à ce qu'il renvoie un code de sortie qui n'est pas 3010, ou jusqu'à ce que le nombre maximum de redémarrage ait été atteint. EC2Launch v2 permet un maximum de 5 redémarrages par tâche. Si vous tentez de redémarrer une instance à partir d'un script à l'aide d'un mécanisme différent, tel que `Restart-Computer`, le statut d'exécution du script sera incohérent. Par exemple, il peut être bloqué dans une boucle de redémarrage ou ne pas effectuer le redémarrage.

Si vous utilisez un format de données utilisateur XML qui est compatible avec les anciens agents, les données utilisateur peuvent s'exécuter plus de fois que vous le souhaitez. Pour plus d'informations, consultez [Le service exécute les données utilisateur plus d'une fois](#) dans la section de résolution des problèmes.

EC2Launch v2 et Sysprep

Le service EC2Launch v2 exécute Sysprep, un outil Microsoft qui vous permet de créer une AMI Windows personnalisée qui peut être réutilisée. Quand EC2Launch v2 appelle Sysprep, il utilise les fichiers présents dans `%ProgramData%\Amazon\EC2Launch` pour déterminer les opérations à effectuer. Vous pouvez modifier ces fichiers indirectement à l'aide de la boîte de dialogue des paramètres EC2Launch ou directement à l'aide d'un éditeur YAML ou d'un éditeur de texte. Toutefois, certains paramètres avancés ne sont pas disponibles dans la boîte de dialogue Propriétés du service EC2Launch ; vous devez donc modifier ces entrées directement.

Si vous créez une AMI directement dans une instance après avoir mis à jour ses paramètres, ceux-ci sont appliqués à n'importe quelle instance lancée dans la nouvelle AMI. Pour plus d'informations sur la création d'une AMI, consultez [Création d'une AMI basée sur Amazon EBS](#).

Dépannage d'EC2Launch v2

Cette section présente les scénarios de dépannage courants pour EC2Launch v2, les informations sur l'affichage des journaux d'événements Windows, ainsi que la sortie et les messages du journal de la console.

Résolution des problèmes liés aux rubriques

- [Scénarios courants de résolution des problèmes](#)
- [Journaux d'événements Windows](#)
- [Sortie du journal de la console EC2Launch v2](#)

Scénarios courants de résolution des problèmes

Cette section présente les scénarios de dépannage courants et les étapes de résolution.

Scénarios

- [Le service ne parvient pas à définir le fond d'écran](#)
- [Le service ne parvient pas à exécuter les données utilisateur](#)
- [Le service exécute une tâche une seule fois](#)
- [Le service ne parvient pas à exécuter une tâche](#)
- [Le service exécute les données utilisateur plus d'une fois](#)
- [Les tâches planifiées à partir d'EC2Launch v1 échouent après la migration vers EC2Launch v2](#)
- [Le service initialise un volume EBS qui n'est pas vide](#)
- [La tâche setWallpaper n'est pas activée, mais le fond d'écran se réinitialise au redémarrage](#)
- [Service bloqué en mode d'exécution](#)
- [agent-config.yml non valide empêche l'ouverture de la boîte de dialogue des paramètres EC2Launch v2](#)
- [task:executeScript should be unique and only invoked once](#)

Le service ne parvient pas à définir le fond d'écran

Résolution

1. Vérifiez si %AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\setwallpaper.lnk existe.
2. Vérifiez dans %ProgramData%\Amazon\EC2Launch\log\agent.log pour voir si des erreurs se sont produites.

Le service ne parvient pas à exécuter les données utilisateur

Cause possible : le service peut avoir échoué avant l'exécution des données utilisateur.

Résolution

1. Vérifiez %ProgramData%\Amazon\EC2Launch\state\previous-state.json.
2. Voyez si boot, network, preReady et postReadyLocalData ont tous été marqués comme une réussite.

3. Si l'une des étapes a échoué, vérifiez si `%ProgramData%\Amazon\EC2Launch\log\agent.log` contient des erreurs spécifiques.

Le service exécute une tâche une seule fois

Résolution

1. Vérifiez la fréquence de la tâche.
2. Si le service a déjà été exécuté après Sysprep et que la fréquence de la tâche est définie sur `once`, la tâche ne s'exécutera plus.
3. Définissez la fréquence de la tâche sur `always` si vous souhaitez qu'elle soit exécutée chaque fois que EC2Launch v2 est exécuté.

Le service ne parvient pas à exécuter une tâche

Résolution

1. Vérifiez les dernières entrées dans `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Si aucune erreur n'est survenue, essayez d'exécuter le service manuellement à partir de `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` pour voir si les tâches réussissent.

Le service exécute les données utilisateur plus d'une fois

Résolution

Les données utilisateur sont traitées différemment entre EC2Launch v1 et EC2Launch v2.

EC2Launch v1 exécute les données utilisateur en tant que tâche planifiée sur l'instance lorsque `persist` est défini sur `true`. Si `persist` est défini sur `false`, la tâche n'est pas planifiée même lorsqu'elle se termine avec un redémarrage ou est interrompue pendant son exécution.

EC2Launch v2 exécute les données utilisateur en tant que tâche d'agent et suit son état d'exécution. Si les données utilisateur entraînent un redémarrage de l'ordinateur ou si leur exécution est interrompue, l'état d'exécution `pending` persiste et les données utilisateur seront réexécutées au démarrage suivant de l'instance. Si vous souhaitez empêcher le script de données utilisateur de s'exécuter plusieurs fois, rendez le script idempotent.

L'exemple suivant de script idempotent définit le nom de l'ordinateur et joint un domaine.

```
<powershell>
$name = $env:computername
if ($name -ne $desiredName) {
Rename-Computer -NewName $desiredName
}
$domain = Get-ADDomain
if ($domain -ne $desiredDomain)
{
Add-Computer -DomainName $desiredDomain
}
$telnet = Get-WindowsFeature -Name Telnet-Client
if (-not $telnet.Installed)
{
Install-WindowsFeature -Name "Telnet-Client"
}
</powershell>
<persist>>false</persist>
```

Les tâches planifiées à partir d'EC2Launch v1 échouent après la migration vers EC2Launch v2

Résolution

L'outil de migration ne détecte aucune tâche planifiée liée aux scripts EC2Launch v1 ; par conséquent, il ne définit pas automatiquement ces tâches dans EC2Launch v2. Pour configurer ces tâches, modifiez le fichier [agent-config.yml](#) ou utilisez la [boîte de dialogue des paramètres d'EC2Launch v2](#). Par exemple, si une tâche planifiée sur une instance exécute `InitializeDisks.ps1`, après avoir exécuté l'outil de migration, vous devez spécifier les volumes que vous souhaitez initialiser dans la boîte de dialogue des paramètres d'EC2Launch v2. Voir l'étape 6 de la procédure pour [Modifier les paramètres à l'aide de la boîte de dialogue des paramètres EC2Launch v2](#).

Le service initialise un volume EBS qui n'est pas vide

Résolution

Avant d'initialiser un volume, EC2Launch v2 tente de détecter s'il est vide. Si un volume n'est pas vide, il ignore l'initialisation. Les volumes détectés comme non vides ne sont pas initialisés. Un volume est considéré comme vide si les 4 premiers Ko d'un volume sont vides ou si un volume n'a pas de [disposition de lecteur reconnaissable par Windows](#). Un volume initialisé et formaté sur un système Linux n'a pas de disposition de lecteur reconnaissable par Windows, par exemple MBR ou GPT. Par conséquent, il sera considéré comme vide et initialisé. Si vous souhaitez conserver

ces données, ne comptez pas sur la détection de lecteurs vides EC2Launch v2. Spécifiez plutôt les volumes que vous souhaitez initialiser dans la [boîte de dialogue des paramètres EC2Launch v2](#) (voir étape 6) ou dans [agent-config.yml](#).

La tâche **setWallpaper** n'est pas activée, mais le fond d'écran se réinitialise au redémarrage

La tâche `setWallpaper` crée le fichier de raccourci `setwallpaper.lnk` dans le dossier de démarrage de chaque utilisateur existant, sauf pour `Default User`. Ce fichier de raccourci s'exécute lorsque l'utilisateur se connecte pour la première fois après le démarrage de l'instance. Il configure l'instance avec un fond d'écran personnalisé qui affiche les attributs de l'instance. La suppression de la tâche `setWallpaper` ne supprime pas ce fichier de raccourci. Vous devez supprimer manuellement ce fichier ou le supprimer à l'aide d'un script.

Le chemin du raccourci est le suivant :

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk
```

Résolution

Supprimez manuellement ce fichier ou supprimez-le à l'aide d'un script.

Exemple de PowerShell script pour supprimer un fichier de raccourci

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
    $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"
    if (Test-Path $startupPath)
    {
        $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
        if (Test-Path $wallpaperSetupPath)
        {
            Remove-Item $wallpaperSetupPath -Force -Confirm:$false
        }
    }
}
```

Service bloqué en mode d'exécution

Description

EC2Launch v2 est bloqué avec des messages de journaux (agent .log) similaires à ce qui suit :

```
2022-02-24 08:08:58 Info:
*****
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Cause possible

SAC est activé et utilise le port série. Pour plus d'informations, consultez [Utilisation de SAC pour dépanner votre instance Windows](#).

Résolution

Essayez les étapes suivantes pour résoudre ce problème :

- Désactivez le service qui utilise le port série.
- Si vous voulez que le service continue à utiliser le port série, écrivez des scripts personnalisés pour exécuter les tâches de l'agent de lancement et invoquez-les en tant que tâches planifiées.

agent-config.yml non valide empêche l'ouverture de la boîte de dialogue des paramètres EC2Launch v2

Description

Les paramètres EC2Launch v2 tentent d'analyser le fichier `agent-config.yml` avant d'ouvrir la boîte de dialogue. Si le fichier de configuration YAML ne suit pas le schéma pris en charge, la boîte de dialogue affiche l'erreur suivante :

```
Unable to parse configuration file agent-config.yml. Review configuration file. Exiting application.
```

Résolution

1. Vérifiez que le fichier de configuration est conforme au [schéma pris en charge](#).

2. Si vous souhaitez commencer à zéro, copiez le fichier de configuration par défaut dans `agent-config.yml`. Vous pouvez utiliser l'[exemple agent-config.yml](#) fourni dans la section Configuration des tâches.
3. Vous pouvez également recommencer en supprimant `agent-config.yml`. Les paramètres EC2Launch v2 génèrent un fichier de configuration vide.

task:executeScript should be unique and only invoked once

Description

Une tâche ne peut pas être répétée dans la même étape.

Résolution

Certaines tâches doivent être entrées sous forme de tableau, telles que [executeScript](#) et [executeProgram](#). Pour obtenir un exemple de la façon d'écrire le script en tant que tableau, consultez [executeScript](#).

Journaux d'événements Windows

EC2Launch v2 publie les journaux des événements Windows pour les événements importants, tels que le démarrage du service, Windows est prêt et la réussite et l'échec des tâches. Les identificateurs d'événement identifient de manière unique un événement particulier. Chaque événement contient des informations sur l'étape, la tâche et le niveau, ainsi qu'une description. Vous pouvez définir des déclencheurs pour des événements spécifiques à l'aide de l'identificateur d'événement.

Les ID d'événement fournissent des informations sur un événement et identifient de manière unique certains événements. Le chiffre le moins significatif d'un ID d'événement indique la gravité d'un événement.

Événement	Chiffre le moins significatif
Success	. . .0
Informational	. . .1
Warning	. . .2

Événement	Chiffre le moins significatif
Error	. . .3

Les événements liés au service qui sont générés au démarrage ou à l'arrêt du service incluent un identifiant d'événement à un seul chiffre.

Événement	Identifiant à un chiffre
Success	0
Informational	1
Warning	2
Error	3

Les messages d'événement pour les événements EC2LaunchService.exe commencent par Service:. Les messages d'événement pour les événements EC2Launch.exe ne commencent pas par Service:.

Les ID d'événement à quatre chiffres incluent des informations sur l'étape, la tâche et la gravité d'un événement.

Rubriques

- [Format de l'ID d'événement](#)
- [Exemples d'ID d'événement](#)
- [Schéma du journal des événements Windows](#)

Format de l'ID d'événement

Le tableau suivant indique le format d'un identificateur d'évènement EC2Launch v2.

3	2 1	0
S	T	L

Les lettres et les chiffres du tableau représentent le type d'événement et les définitions suivants.

Type d'événement	Définition
S (Stage)	0 - Message de niveau de service 1 - Démarrer 2 - Réseau 3 - PreReady 5 - Windows est prêt 6 - PostReady 7 - Données utilisateur
T (Tâche)	Les tâches représentées par les deux valeurs correspondantes sont différentes pour chaque étape. Pour afficher la liste complète des événements, consultez Schéma du journal des événements Windows .
L (Niveau de l'événement)	0 - Réussite 1 - Informationnel 2 - Avertissement 3 - Erreur

Exemples d'ID d'événement

Voici des exemples d'ID d'événement.

- 5000 - Windows est prêt à l'emploi
- 3010- La tâche d'activation de Windows en cours d' PreReady étape a été réussie

- 6013- La tâche de définition du fond d'écran dans le stage PostReady Local Data a rencontré une erreur

Schéma du journal des événements Windows

MessageId/Identifiant de l'événement	Message d'événement
. . .0	Success
. . .1	Informational
. . .2	Warning
. . .3	Error
x	EC2Launch service-level logs
0	EC2Launch service exited successfully
1	EC2Launch service informational logs
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)

MessageId/Identifiant de l'événement	Message d'événement
1000	Boot
1010	Boot - extend_root_partition
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper

MessageId/Identifiant de l'événement	Message d'événement
6020/7020	PostReadyLocal/UserData - set_update_schedule
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_op en_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

Sortie du journal de la console EC2Launch v2

Cette section contient un exemple de sortie du journal de la console pour EC2Launch v2 et répertorie tous les messages d'erreur du journal de la console EC2Launch v2 pour vous aider à résoudre les problèmes. Pour plus d'informations sur la sortie de la console d'instance et sur la manière d'y accéder, consultez [the section called "Sortie de la console de l'instance"](#).

Outputs

- [Sortie du journal de la console EC2Launch v2](#)
- [Messages du journal de la console EC2Launch v2](#)

Sortie du journal de la console EC2Launch v2

Voici un exemple de sortie du journal de la console pour EC2Launch v2.

```
2023/11/30 20:18:53Z: Windows sysprep configuration complete.
2023/11/30 20:18:57Z: Message: Waiting for access to metadata...
2023/11/30 20:18:57Z: Message: Meta-data is now available.
2023/11/30 20:18:57Z: AMI Origin Version: 2023.11.15
2023/11/30 20:18:57Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2023/11/30 20:18:58Z: OS: Microsoft Windows NT 10.0.20348
2023/11/30 20:18:58Z: OsVersion: 10.0
2023/11/30 20:18:58Z: OsProductName: Windows Server 2022 Datacenter
2023/11/30 20:18:58Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2023/11/30 20:18:58Z: OsCurrentBuild: 20348
2023/11/30 20:18:58Z: OsReleaseId: 2009
2023/11/30 20:18:58Z: Language: en-US
2023/11/30 20:18:58Z: TimeZone: UTC
2023/11/30 20:18:58Z: Offset: UTC +0000
2023/11/30 20:18:58Z: Launch: EC2 Launch v2.0.1643
2023/11/30 20:18:58Z: AMI-ID: ami-1234567890abcdef1
2023/11/30 20:18:58Z: Instance-ID: i-1234567890abcdef0
2023/11/30 20:18:58Z: Instance Type: c5.large
2023/11/30 20:19:00Z: Driver: AWS NVMe Driver v1.5.0.33
2023/11/30 20:19:00Z: SubComponent: AWS NVMe Driver v1.5.0.33;
  EnableSCSIPersistentReservations: 0
2023/11/30 20:19:00Z: Driver: AWS PV Driver Package v8.4.3
2023/11/30 20:19:01Z: Driver: Amazon Elastic Network Adapter v2.6.0.0
2023/11/30 20:19:01Z: RDPCERTIFICATE-SUBJECTNAME: EC2AMAZ-S01T009
2023/11/30 20:19:01Z: RDPCERTIFICATE-THUMBPRINT:
  1234567890ABCDEF1234567890ABCDEF1234567890
2023/11/30 20:19:09Z: SSM: Amazon SSM Agent v3.2.1705.0
2023/11/30 20:19:13Z: Username: Administrator
2023/11/30 20:19:13Z: Password: <Password>
1234567890abcdef1EXAMPLEPASSWORD
</Password>
2023/11/30 20:19:14Z: User data format: no_user_data
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
```

```
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
2023/11/30 20:19:14Z: Message: Windows is Ready to use
```

Messages du journal de la console EC2Launch v2

Voici une liste de tous les messages du journal de la console EC2Launch v2.

```
Message: Error EC2Launch service is stopping. {error message}
  Error setting up EC2Launch agent folders
  See instance logs for detail
  Error stopping service
  Error initializing service
Message: Windows sysprep configuration complete
Message: Invalid administrator username: {invalid username}
Message: Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
Microsoft-Hyper-V is installed.
Unable to get service status for vmms
Microsoft-Hyper-V is {status}
SSM: Amazon SSM Agent {version}
```

```

AWS VSS Version: {version}
Message: Windows sysprep configuration complete
Message: Windows is being configured. SysprepState is {state}
Windows is still being configured. SysprepState is {state}
Message: Windows is Ready to use
Message: Waiting for meta-data accessibility...
Message: Meta-data is now available.
Message: Still waiting for meta-data accessibility...
Message: Failed to find primary network interface...retrying...
User data format: {format}

```

Historique des versions EC2Launch v2

Historique des versions

- [Historique des versions EC2Launch v2](#)
- [Historique des versions de l'outil de migration EC2Launch v2](#)

Historique des versions EC2Launch v2

Le tableau suivant décrit les versions publiées d'EC2Launch v2.

Version	Détails	Date de publication
2,0,1924	<ul style="list-style-type: none"> • Mise à jour de l'interface utilisateur des paramètres d'EC2Launch. • Mise à jour de la commande CLI du fond d'écran. • Mise à jour du programme d'installation d'EC2Launch. 	10 juin 2024
2,0,114	<ul style="list-style-type: none"> • Ajoutez des itinéraires avec des adresses de passerelle non spécifiées (0.0.0.0 pour IPv4 ou :: pour IPv6). • Ajoutez toujours des routes IPv4 et IPv6. • 	5 juin 2024

Version	Détails	Date de publication
	<p>Correction d'un problème en raison duquel le nom Administrator d'utilisateur était ajouté au agent-config.yml fichier alors qu'il n'était pas spécifié.</p> <ul style="list-style-type: none"> • Permissions EC2Launch v2 modifiées. 	
2,0,1881	<ul style="list-style-type: none"> • Ajout d'une option de mot de passe crypté à setAdminAccount la tâche. • Ajout de la commande CLI pour chiffrer le mot de passe statique dans agent-config.yml. • Correction d'un problème en raison duquel les données utilisateur XML n'ajoutaient pas d' PowerShell arguments lorsqu'elles étaient exécutées avec des autorisations d'administrateur. Pour en savoir plus, consultez Comment Amazon EC2 gère les données utilisateur pour les instances Windows. • PowerShell Arguments ajustés pour les scripts de executeScript tâche et de données utilisateur lorsqu'ils sont exécutés avec LocalSystem des autorisations. Lorsque les arguments sont vides, l'agent utilise la valeur par défaut suivante :-ExecutionPolicy Unrestricted . • Impossible d'imprimer des versions de pilotes dupliquées dans le journal de la console. 	8 mai 2024

Version	Détails	Date de publication
2,0,115	<ul style="list-style-type: none">• Gestion des erreurs ajustée pour échouer en cas de problèmes de configuration critiques avant Sysprep.• Correction d'un problème en raison duquel les tâches de fond d'écran et de nom d'hôte pouvaient utiliser une adresse IP incorrecte sur les instances où plusieurs adresses IP étaient attribuées à l'interface réseau principale.• Les tâches de fond d'écran et de nom d'hôte ont d'abord été modifiées pour obtenir une adresse IP privée depuis l'IMDS, puis pour revenir à WMI si l'IMDS est désactivé.• Correction d'un problème lié à la <code>initializeVolume</code> tâche qui <code>sc1</code> empêchait l'initialisation des volumes en raison d'une erreur transitoire.	6 mars 2024
2,0,1739	<ul style="list-style-type: none">• Correction d'un problème qui empêchait les codes de sortie d'être capturés par <code>executeScript</code> des tâches exécutées en tant qu'administrateur Windows.	17 janvier 2024

Version	Détails	Date de publication
2,0,1702	<ul style="list-style-type: none">• Autorisations <code>Telemetry.log</code> limitées de <code>read-execute</code> uniquement pour les utilisateurs standard.• Configuration du service Windows <code>EC2Launch</code> pour qu'il redémarre en cas d'échec du démarrage.• Défaillances <code>add-routes</code> rendues exploitables en enregistrant les résultats <code>route.exe stderr</code>.• Correction d'un problème qui se produisait lorsque les métriques d'itinéraire se situaient en dehors de la plage [1-9999].• Ajout de la prise en charge du fond d'écran à plusieurs nouveaux types d'instance.• Correction d'un problème causé par les scripts de données utilisateur qui s'exécutaient en tant qu'utilisateur administrateur Windows et envoyaient des résultats à <code>stderr</code>.	4 janvier 2024

Version	Détails	Date de publication
2,0,1643	<ul style="list-style-type: none">• Mise à jour de l'outil <code>ebsnvme-id.exe</code> vers la version 1.1.0.7.• Correction d'un problème lié aux paramètres de dimensionnement côté réception (RSS) et de profondeur de file d'attente de réception sur les types d'instance metal commençant par « metal-* », telle que metal-48x1.• Suppression de l'événement de télémétrie signalant les commandes XML de données utilisateur qui bloquent l'agent.• Mise à jour de la tâche <code>setDnsSuffix</code> pour limiter la dévolution des noms de domaine en fonction de l'entrée dans le registre <code>:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel</code>.• Ajout d'une tâche publique et d'une CLI qui ajoutent des routes réseau.• Remarque : cette version est officiellement la dernière à être compatible avec Windows Server 2012.• Remarque : cette version est officiellement la dernière à être compatible avec les systèmes d'exploitation 32 bits.	4 octobre 2023
2,0,1580	<ul style="list-style-type: none">• Modification de la façon dont l'agent de lancement gère les erreurs lorsque vous modifiez les autorisations du fichier journal.• Ajout d'un délai d'attente pour la connexion au port série. Le délai d'attente permet à l'agent de lancement de continuer à fonctionner si le port série est utilisé.	5 septembre 2023

Version	Détails	Date de publication
2,0,1521	<ul style="list-style-type: none">• L'indicateur <code>-block</code> des commandes <code>EC2Launch.exe</code>, <code>reset</code> et <code>sysprep</code> est devenu obsolète.• Mise à jour de <code>EC2Launch.exe</code> pour détecter et gérer les commandes <code>reset</code> et <code>sysprep</code> utilisées dans les tâches <code>executeScript</code> en ligne. Ces commandes interrompent l'exécution de l'agent une fois la tâche <code>executeScript</code> exécutée.• Les scripts de données utilisateur XML ont été mis à jour pour s'exécuter en ligne par défaut.• Autorisez les scripts de données utilisateur XML à s'exécuter séparément avec la nouvelle balise <code>detach</code>. Pour en savoir plus, consultez Scripts de données utilisateur.• A apporté les modifications suivantes au journal de l'agent.<ul style="list-style-type: none">• Messages du journal de l'agent mis à jour.• Contenu <code>executeScript</code> et sortie supprimés du journal de l'agent.• Arguments <code>executeProgram</code> et sortie supprimés du journal de l'agent.• A apporté les modifications suivantes au journal de la console.<ul style="list-style-type: none">• Valeur <code>EnableSCSIPersistentReservations</code> ajoutée au journal de la console.	3 juillet 2023

Version	Détails	Date de publication
2,0.1303	<ul style="list-style-type: none">• Ajout d'une gestion des erreurs et de lignes de journal supplémentaires lors de l'ajout d'itinéraires réseau.• <code>executeScript</code> Autorisés et <code>executeProgram</code> tâches en cours de PreReady stage.• Mise à jour de la tâche <code>executeProgram</code> pour générer des fichiers de sortie similaires à ceux de la tâche <code>executeScript</code>. Pour plus d'informations, consultez executeProgram.• Ajout d'une télémétrie pour surveiller l'utilisation des commandes de l'agent de blocage dans les données utilisateur XML.	3 mai 2023
2,0.1245	<ul style="list-style-type: none">• Visibilité améliorée des incidents en enregistrant les piles d'appels d'incidents en texte clair.• Le EventLog service a été ajouté en tant que dépendance au démarrage pour corriger un crash lorsque le service Amazon EC2Launch démarre plus rapidement que le EventLog service.• Les données utilisateur XML ont été exécutées avant l' PostReady étape à partir du fichier de configuration de l'agent (comme EC2Launch v1 et EC2Config).• Ajout de la version 1.1 des données utilisateur YAML pour que les données utilisateur soient exécutées avant l' PostReady étape à partir du fichier de configuration de l'agent (les données utilisateur YAML version 1.0 s'exécutent après l' PostReady étape à partir du fichier de configuration de l'agent).	8 mars 2023

Version	Détails	Date de publication
2,0.1173	<ul style="list-style-type: none">• Ajoute une fonction facultative pour afficher les balises d'instance sur le fond d'écran. Pour plus d'informations, consultez setWallpaper .• Ajoute la gestion des erreurs lorsque le groupe de sécurité pour Elastic Graphics n'est pas correctement configuré.• Corrige un délai d'expiration lorsque le service de métadonnées d'instance n'est pas activé.	6 février 2023
2,0.1121	<ul style="list-style-type: none">• Résout un problème où une erreur 404 est imprimée sur le fond d'écran quand aucune adresse IPv4 publique n'est attribuée.• Corrige un problème où le système de fichiers du volume est formaté en RAW au lieu de NTFS lorsque la lettre de lecteur de son périphérique est définie sur D.• Corrige un problème dans lequel les volumes SSD NVMe sont incorrectement identifiés en tant que volumes EBS.• Corrige une erreur lors de l'activation de Windows lorsque l'IMDS est désactivé.	4 janvier 2023

Version	Détails	Date de publication
2,0.1082	<ul style="list-style-type: none">• Corrige un problème selon lequel le champ <code>setWallpaper : privateIpAddress</code> est vide lorsque IMDS est désactivé.• Résout un problème lié à la définition du nom d'hôte sur l'adresse IPv4 privée lorsque IMDS est désactivé.• Corrige un problème lié à l'initialisation des volumes sous Windows Server 2012.• Corrige un problème lié à la définition des trames Jumbo.• Corrige un problème selon lequel aucune clé SSH n'est spécifiée au lancement de l'instance.• Corrige une erreur sur Windows Server 2012 lorsque Windows ne possède pas de clé de registre <code>Releaseld</code> « ».	7 décembre 2022
2,0.1011	<ul style="list-style-type: none">• Corrige la logique de recherche de l'adaptateur réseau lorsque <code>PnPDeviceID</code> est vide.	11 novembre 2022
2,0.1009	<ul style="list-style-type: none">• Utilise les informations du segment PCI pour sélectionner le port de la console.	8 novembre 2022

Version	Détails	Date de publication
2,0.982	<ul style="list-style-type: none">• Ajoute une logique de nouvelle tentative pour obtenir des informations RDP.• Corrige les erreurs lors de l'initialisation du volume sur les instances d2.8xlarge .• Corrige les problèmes liés à la sélection d'une carte réseau incorrecte après un redémarrage.• Supprime le message d'erreur de fausse alarme lorsque ACPI SPCR n'est pas disponible.	31 octobre 2022
2,0.863	<ul style="list-style-type: none">• Met à jour la logique d'attente IMDS pour effectuer uniquement des requêtes IMDSv2.• Ajoute une logique pour attribuer une lettre de lecteurs aux volumes déjà initialisés, mais non montés.• Affiche un message d'erreur plus spécifique lorsque le type de paire de clés n'est pas pris en charge.• Corrige le bogue de code de redémarrage 3010.• Ajoute la vérification de la validité des données utilisateur encodées en base64.	6 juillet 2022
2,0,698	<ul style="list-style-type: none">• Corrige la faute d'orthographe dans la sortie du journal lors de l'exécution de scripts.	30 janvier 2022

Version	Détails	Date de publication
2,0,674	<ul style="list-style-type: none">• La télémétrie charge le contrôle de confidentialité activé/désactivé.• Corrige le bogue <code>index out of bounds</code>.• Supprime les raccourcis de fond d'écran pendant <code>sysprep</code>.	15 novembre 2021
2,0,651	<ul style="list-style-type: none">• Ajoute une logique permettant de désinstaller les agents hérités pendant l'installation d'EC2Launch v2.• Corrige le problème de CLI <code>list-volume</code> lorsque le volume racine n'est pas répertorié en tant que volume 0.	7 octobre 2021
2,0,592	<ul style="list-style-type: none">• Corrige un bug pour signaler correctement l'état de l'étape.• Supprime les faux messages d'alarme lorsque les fichiers journaux sont fermés.• Ajoute la télémétrie.	31 août 2021
2,0,548	<ul style="list-style-type: none">• Ajout de zéros de début pour le nom d'hôte IP hexadécimal• Correction des autorisations de fichier pour la tâche <code>enableOpenSsh</code>.• Correction du plantage de la commande <code>sysprep</code>.	4 août 2021

Version	Détails	Date de publication
2,0,470	<ul style="list-style-type: none">• Correction d'un bug dans la phase réseau qui attendait que DHCP attribue une adresse IP à l'instance.• Correction d'un bug avec <code>setDnsSuffix</code> lorsque la clé de registre <code>SearchList</code> n'existe pas.• Correction d'un bug dans la logique de transfert DNS dans <code>setDnsSuffix</code>.• Ajout des itinéraires réseau après les redémarrages intermédiaires.• Autorise <code>initializeVolume</code> à réécrire les volumes existants.• Supprime les informations supplémentaires de la sous-commande de version.	20 juillet 2021
2.0.285	<ul style="list-style-type: none">• Ajoute une option pour exécuter des scripts utilisateur dans un processus détaché.• Les données utilisateur héritées (données utilisateur XML) s'exécutent désormais dans un processus détaché, ce qui est similaire à celui de l'agent de lancement précédent.• Ajoute l'indicateur CLI aux commandes <code>sysprep</code> et <code>reset</code>, ce qui leur permet de bloquer jusqu'à ce que le service s'arrête.• Restreint les autorisations du dossier de configuration.	8 mars 2021

Version	Détails	Date de publication
2.0.207	<ul style="list-style-type: none">• Ajoute un champ <code>hostName</code> facultatif à la tâche <code>setHostName</code> .• Correction du bogue de redémarrage. Les tâches de redémarrage <code>executeScript</code> et <code>executeProgram</code> seront marquées comme étant en cours d'exécution.• Ajoute d'autres codes de retour à la commande d'état.• Ajoute un service d'amorçage pour résoudre le problème de démarrage lors de l'exécution sur le type d'instance <code>t2.nano</code>.• Corrige le mode d'installation propre pour supprimer les fichiers non suivis par le programme d'installation.	2 février 2021
2.0.160	<ul style="list-style-type: none">• Corrige la commande <code>validate</code> pour qu'elle détecte les noms d'étape non valides.• Ajoute la commande <code>w32tm resync</code> dans la tâche <code>addroutes</code> .• Résolution d'un problème lié à la modification de l'ordre de recherche du suffixe DNS• Ajoute des conditions de vérification pour mieux signaler les données utilisateur invalides.	4 décembre 2020
2.0.153	Ajoute la fonctionnalité Sysprep dans. <code>UserData</code>	3 novembre 2020

Version	Détails	Date de publication
2.0.146	<ul style="list-style-type: none">• Résout un problème lié RootExtend aux AMI non anglophones.• Donne aux utilisateurs l'autorisation d'écriture de groupe pour les fichiers journaux.• Crée une partition MS Reserved pour les volumes GPT.• Ajoute une commande list-volumes et la liste déroulante des volumes dans les paramètres Amazon EC2Launch.• Ajoute une get-agent-config commande pour imprimer le fichier agent-config.yml au format yaml ou json.• Efface le mot de passe statique si aucune clé publique n'a été détectée.	6 octobre 2020
2.0.124	<ul style="list-style-type: none">• Ajoute l'option pour afficher la version du système d'exploitation sur le fond d'écran.• Initialise les volumes EBS chiffrés.• Ajoute des routes pour les VPC sans nom DNS local.	10 septembre 2020
2.0.104	<ul style="list-style-type: none">• Crée une liste de recherche de suffixe DNS si elle n'existe pas déjà.• Ignore la mise en veille prolongée si elle n'est pas demandée.	12 août 2020
2.0.0	Première version.	30 juin 2020

Historique des versions de l'outil de migration EC2Launch v2

Le tableau suivant décrit les versions publiées de l'outil de migration EC2Launch v2.

Version	Détails	Date de publication
1,0396	<ul style="list-style-type: none">• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1924.	11 juin 2024
1,0394	<ul style="list-style-type: none">• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1914.	6 juin 2024
1,0,384	<ul style="list-style-type: none">• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1881.	8 mai 2024
1,0,358	<ul style="list-style-type: none">• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1815.	8 mars 2024
1,0345	<ul style="list-style-type: none">• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1739.	18 janvier 2024
1,0342	<ul style="list-style-type: none">• Mettez à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1702.	5 janvier 2024
1,0,331	<ul style="list-style-type: none">• Mise à jour de l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1643.• Correction d'une erreur qui se produit lors de l'exécution de <code>.Install.ps1 -DryRun</code>.• Correction d'un problème où la configuration du mot de passe est incorrectement définie sur <code>random</code> lors de la migration depuis EC2Config.•	3 novembre 2023

Version	Détails	Date de publication
	Correction d'une erreur qui se produit si <code>setWallpaper</code> est défini sur <code>False</code> lors de la migration depuis EC2Launch.	
1,0,303	Met à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1580.	14 septembre 2023
1,0,286	Met à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1521.	14 juillet 2023
1,0,272	Met à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1303.	3 mai 2023
1,0,262	Met à jour l'outil de migration avec la dernière version de l'agent EC2Launch v2 : 2.0.1245.	9 mars 2023
1,0,241	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.1011.	7 décembre 2022
1,0,218	<ul style="list-style-type: none"> • Valide la valeur de région extraite des métadonnées de l'instance. • Corrige un bogue d'échec de migration dans les modules linguistiques. • Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.863. 	3 septembre 2022
1,0162	<ul style="list-style-type: none"> • Déplace la logique de suppression des agents hérités vers le MSI EC2Launch v2. • Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.698. 	18 mars 2022
100,136	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.651.	13 octobre 2021

Version	Détails	Date de publication
100,130	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.548.	5 août 2021
100,113	Utilise IMDSv2 à la place d'IMDSv1.	4 juin 2021
1.0.101	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.285.	12 mars 2021
1.0.86	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.207.	3 février 2021
1.0.76	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.160.	4 décembre 2020
1.0.69	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.153.	5 novembre 2020
1.0.65	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.146.	9 octobre 2020
1.0.60	Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.124.	10 septembre 2020
1.0.54	<ul style="list-style-type: none"> • Installe EC2Launch v2 si aucun agent n'est installé. • Incrémente le numéro de version de l'agent EC2Launch v2 à 2.0.104. • Découple SSM Agent. 	12 août 2020
1.0.50	Supprime NuGet la dépendance.	10 août 2020
1.0.0	Première version.	30 juin 2020

Configurer une instance Windows à l'aide d'EC2Launch

EC2Launch est un ensemble de PowerShell scripts Windows qui ont remplacé le service EC2Config sur les AMI Windows Server 2016 et 2019. Beaucoup de ces AMI sont encore disponibles.

EC2Launch v2 est le dernier agent de lancement pour toutes les versions Windows prises en charge, qui remplace à la fois EC2Config et EC2Launch. Pour plus d'informations, consultez [Configurer une instance Windows à l'aide d'EC2Launch v2](#).

Note

Pour utiliser EC2Launch avec IMDSv2, la version doit être 1.3.2002730 ou ultérieure.

Table des matières

- [Tâches EC2Launch](#)
- [Télémétrie](#)
- [Installer la version la plus récente d'EC2Launch](#)
- [Vérification de la version d'EC2Launch](#)
- [Structure du répertoire EC2Launch](#)
- [Configurer EC2Launch](#)
- [Historique des versions EC2Launch](#)

Tâches EC2Launch

EC2Launch effectue les tâches suivantes par défaut pendant le démarrage initial de l'instance :

- Configure un nouveau fond d'écran qui présente les informations relatives à l'instance.
- Définit le nom de l'ordinateur sur l'adresse IPv4 privée de l'instance.
- Envoie les informations d'instance à la console Amazon EC2.
- Envoie l'empreinte numérique du certificat RDP à la console EC2.
- Définit un mot de passe aléatoire pour le compte d'administrateur.
- Ajoute des suffixes DNS.
- Etend de manière dynamique la partition du système d'exploitation pour inclure l'espace non partitionné.

- Exécute les données utilisateur (si spécifié). Pour plus d'informations sur la spécification de données utilisateur, consultez [Utiliser les données utilisateur d'instance](#).
- Définit des itinéraires statiques persistants pour atteindre le service de métadonnées et AWS KMS les serveurs.

Important

Si une AMI personnalisée est créée à partir de cette instance, ces routes sont capturées dans le cadre de la configuration du système d'exploitation et toutes les nouvelles instances lancées à partir de cette AMI conserveront les mêmes routes, quel que soit leur placement sur le sous-réseau. Pour mettre à jour les routes, consultez [Mettre à jour les routes des métadonnées/serveurs KMS pour Server 2016 et versions ultérieures lors du lancement d'une AMI personnalisée](#).

Les tâches suivantes contribuent à assurer la rétrocompatibilité avec le service EC2Config. Vous pouvez également configurer EC2Launch pour réaliser ces tâches au moment du démarrage :

- Initialiser des volumes EBS secondaires.
- Envoyer des journaux d'événements Windows aux journaux de console EC2
- Envoyer le message Windows is ready to use (Windows est prêt à être utilisé) à la console EC2

Pour plus d'informations concernant Windows Server 2019, consultez la page relative à la [comparaison des fonctions dans les versions de Windows Server](#) sur Microsoft.com.

Télémetrie

La télémétrie est une information supplémentaire qui permet de mieux AWS comprendre vos besoins, de diagnostiquer les problèmes et de fournir des fonctionnalités pour améliorer votre expérience avec AWS les services.

La version EC2Launch 1.3.2003498 et les versions ultérieures collectent les données de télémétrie, comme les métriques d'utilisation et les erreurs. Ces données sont collectées à partir de l'instance Amazon EC2 sur laquelle s'exécute EC2Launch. Cela inclut toutes les AMI Windows détenues par AWS.

Les types de données télémétriques suivants sont collectés par EC2Launch :

- Usage information (Informations d'utilisation) : commandes de l'agent, méthode d'installation et fréquence d'exécution planifiée.
- Errors and diagnostic information (Erreurs et informations de diagnostic) : installation de l'agent et exécution des codes d'erreur.

Exemples de données collectées :

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

La télémétrie est activée par défaut. Vous pouvez désactiver la collecte de données de télémétrie à tout moment. Si la télémétrie est activée, EC2Launch v2 envoie des données de télémétrie sans notifications supplémentaires au client.

Le choix d'activer ou de désactiver la télémétrie est collecté.

Vous pouvez choisir de vous inscrire ou de vous désinscrire de la collecte de télémétrie. Votre choix est collecté afin de nous assurer que nous le respectons.

Visibilité de la télémétrie

Lorsque la télémétrie est activée, elle apparaît dans la sortie de la console Amazon EC2 comme suit :

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Désactiver la télémétrie sur une instance

Pour désactiver la télémétrie en paramétrant une variable d'environnement système, exécutez la commande suivante en tant qu'administrateur :

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Pour désactiver la télémétrie pendant l'installation, exécutez `install.ps1` comme suit :

```
. .\install.ps1 -EnableTelemetry:$false
```

Installer la version la plus récente d'EC2Launch

Utilisez la procédure suivante pour télécharger et installer manuellement la version la plus récente d'EC2Launch sur vos instances.

Pour télécharger et installer la version la plus récente d'EC2Launch

1. Si vous avez déjà installé et configuré EC2Launch sur une instance, effectuez une sauvegarde du fichier de configuration EC2Launch. Le processus d'installation ne conserve pas les modifications de ce fichier. Par défaut, le fichier se trouve dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Téléchargez [EC2-Windows-Launch.zip](#) dans un répertoire sur l'instance.
3. Téléchargez [install.ps1](#) dans le répertoire dans lequel vous avez téléchargé `EC2-Windows-Launch.zip`.
4. Exécutez `install.ps1`
5. Si vous avez effectué une sauvegarde du fichier de configuration EC2Launch, copiez-la dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Pour télécharger et installer la dernière version d'EC2Launch à l'aide de PowerShell

Si vous avez déjà installé et configuré EC2Launch sur une instance, effectuez une sauvegarde du fichier de configuration EC2Launch. Le processus d'installation ne conserve pas les modifications de ce fichier. Par défaut, le fichier se trouve dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Pour installer la dernière version d'EC2Launch à l'aide de PowerShell, exécutez les commandes suivantes depuis une fenêtre PowerShell

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-Launch.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $url - Leaf)
Invoke-WebRequest -Uri $url -OutFile $DownloadZipFile
$url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $url - Leaf)
Invoke-WebRequest -Uri $url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

Note

Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016, il est possible que le protocole TLS 1.2 doive être activé sur votre PowerShell terminal. Vous pouvez activer le protocole TLS 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Vérifiez l'installation en vérifiant `C:\ProgramData\Amazon\EC2-Windows\Launch`.

Vérification de la version d'EC2Launch

Utilisez la PowerShell commande Windows suivante pour vérifier la version installée d'EC2Launch.

```
PS C:\> Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psd1" | Select Version
```

Structure du répertoire EC2Launch

EC2Launch est installé par défaut sur les AMI Windows Server 2016 et versions ultérieures dans le répertoire racine `C:\ProgramData\Amazon\EC2-Windows\Launch`.

Note

Par défaut, Windows masque les fichiers et les dossiers qui se trouvent sous `C:\ProgramData`. Pour afficher les fichiers et les répertoires EC2Launch, vous devez taper le chemin d'accès dans l'Explorateur Windows ou modifier les propriétés de dossier afin d'afficher les fichiers et les dossiers masqués.

Le répertoire Launch contient les sous-répertoires suivants.

- **Scripts**— Contient les PowerShell scripts qui composent EC2Launch.
- **Module** — Contient le module pour créer des scripts liés à Amazon EC2.
- **Config** — Contient les fichiers de configuration de script que vous pouvez personnaliser.

- **Sysprep** — Contient les ressources Sysprep.
- **Settings** — Contient une application pour l'interface utilisateur graphique de Sysprep.
- **Library**—Contient des bibliothèques partagées pour les agents de lancement EC2.
- **Logs** — Contient les fichiers journaux générés par des scripts.

Version EC2Launch et versions ultérieures **1.3.2004592**

Les utilisateurs du Administrators groupe sont autorisés à accéder à Full control tous les annuaires EC2Launch. Les utilisateurs qui ne font pas partie du groupe des administrateurs sont autorisés à accéder à Read & execute tous les annuaires EC2Launch, sauf. C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Config L'Configannuaire est réservé aux utilisateurs membres du Administrators groupe.

Version EC2Launch et versions antérieures **1.3.2004491**

Tous les répertoires EC2Launch héritent de leurs autorisations, sauf. C:\ProgramData C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Scripts Ce dossier hérite de toutes les autorisations C:\ProgramData initiales depuis sa création, mais empêche les utilisateurs normaux d'accéder CreateFiles au répertoire.

Configurer EC2Launch

Lorsque votre instance a été initialisée pour la première fois, vous pouvez configurer EC2Launch pour s'exécuter à nouveau et effectuer des tâches de start-up distinctes.

Tâches

- [Configuration des tâches d'initialisation](#)
- [Planification d'EC2Launch pour exécution lors de chaque démarrage](#)
- [Initialisation des disques et mappage des lettres de lecteur](#)
- [Envoi des journaux d'événements Windows à la console EC2](#)
- [Envoi du message « Windows Is Ready » après un démarrage réussi](#)

Configuration des tâches d'initialisation

Spécifiez les paramètres dans le fichier LaunchConfig.json pour activer ou désactiver les tâches d'initialisation suivantes :

- Définissez le nom d'ordinateur sur l'adresse IPv4 privée de l'instance.
- Réglez le moniteur pour qu'il reste toujours en fonction.
- Configurer un nouveau fond d'écran
- Ajouter une liste de suffixes DNS

Note

Cela ajoute une recherche de suffixe DNS pour le domaine suivant et configure d'autres suffixes standard. Pour plus d'informations sur la façon dont les agents de lancement définissent les suffixes DNS, consultez. [Configurer le suffixe DNS pour les agents de lancement Windows](#)

```
region.ec2-utilities.amazonaws.com
```

- Elargir la taille de volume de démarrage
- Définir le mot de passe de l'administrateur

Pour configurer les paramètres d'initialisation

1. Dans l'instance à configurer, ouvrez le fichier suivant C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json dans un éditeur de texte.
2. Mettez à jour les paramètres suivants au besoin et enregistrez vos modifications. Indiquez un mot de passe dans adminPassword uniquement si adminPasswordtype est Specify.

```
{
  "setComputerName": false,
  "setMonitorAlwaysOn": true,
  "setWallpaper": true,
  "addDnsSuffixList": true,
  "extendBootVolumeSize": true,
  "handleUserData": true,
  "adminPasswordType": "Random | Specify | DoNothing",
  "adminPassword": "password that adheres to your security policy (optional)"
}
```

Les types de mots de passe sont définis comme suit :

Random

EC2Launch génère un mot de passe et le chiffre à l'aide de la clé de l'utilisateur. Le système désactive ce paramètre après le lancement de l'instance afin que ce mot de passe persiste si l'instance est redémarrée, arrêtée ou démarrée.

Specify

EC2Launch utilise le mot de passe que vous spécifiez dans `adminPassword`. Si ce mot de passe ne répond pas aux exigences du système, EC2Launch génère un mot de passe aléatoire à la place. Le mot de passe est stocké dans le fichier `LaunchConfig.json` sous forme de texte clair et est supprimé une fois que le mot de passe est défini par Sysprep. EC2Launch chiffre le mot de passe à l'aide de la clé de l'utilisateur.

DoNothing

EC2Launch utilise le mot de passe que vous spécifiez dans le fichier `unattend.xml`. Si vous ne spécifiez pas de mot de passe dans `unattend.xml`, le compte d'administrateur est désactivé.

3. Dans Windows PowerShell, exécutez la commande suivante pour planifier l'exécution du script en tant que tâche planifiée Windows. Le script s'exécute une seule fois lors du prochain démarrage, puis désactive toute nouvelle exécution de ces tâches.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 - Schedule
```

Planification d'EC2Launch pour exécution lors de chaque démarrage

Vous pouvez planifier l'exécution d'EC2Launch lors de chaque démarrage plutôt que seulement lors du démarrage initial.

Pour activer l'exécution d'EC2Launch lors de chaque démarrage :

1. Ouvrez Windows PowerShell et exécutez la commande suivante :

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 - SchedulePerBoot
```

2. Ou exécutez le fichier exécutable avec la commande suivante :

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

Ensuite, sélectionnez `Run EC2Launch on every boot`. Vous pouvez spécifier `Shutdown without Sysprep` ou `Shutdown with Sysprep` pour votre instance EC2.

Note

Lorsque vous activez l'exécution d'EC2Launch à chaque démarrage, voici ce qui se produira lors de la prochaine exécution d'EC2Launch :

- Si `AdminPasswordType` est toujours défini sur `Random`, EC2Launch générera un nouveau mot de passe au prochain démarrage. Après ce démarrage, `AdminPasswordType` est automatiquement défini sur `DoNothing` pour empêcher EC2Launch de générer de nouveaux mots de passe lors des démarrages suivants. Pour empêcher EC2Launch de générer un nouveau mot de passe lors du premier démarrage, définissez manuellement `AdminPasswordType` sur `DoNothing` avant de redémarrer.
- `HandleUserData` sera redéfini sur `false` sauf si `persist` est défini sur `true` pour les données utilisateur. Pour plus d'informations, consultez [the section called "Scripts de données utilisateur"](#).

Initialisation des disques et mappage des lettres de lecteur

Spécifiez les paramètres dans le fichier `DriveLetterMappingConfig.json` pour mapper les lettres de lecteur avec les volumes appropriés de votre instance EC2. Le script initialise les lecteurs qui ne sont pas encore initialisés et partitionnés. Pour plus d'informations sur l'obtention de détails sur les volumes sous Windows, veuillez consulter [Get-Volume](#) (français non garanti) dans la documentation Microsoft.

Pour mapper les lettres de lecteur avec les volumes

1. Ouvrez le fichier `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` dans un éditeur de texte.
2. Spécifiez les paramètres de volume suivants et enregistrez vos modifications :

```
{  
  "driveLetterMapping": [  
    {
```

```
{
  "volumeName": "sample volume",
  "driveLetter": "H"
}
]
```

3. Ouvrez Windows PowerShell et utilisez la commande suivante pour exécuter le script EC2Launch qui initialise les disques :

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Pour initialiser les disques chaque fois que l'instance démarre, ajoutez l'indicateur `-Schedule` comme suit :

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

Envoi des journaux d'événements Windows à la console EC2

Spécifiez les paramètres dans le fichier de `EventLogConfig.json` afin d'envoyer les journaux d'événements Windows aux journaux de la console EC2.

Pour configurer les paramètres permettant d'envoyer les journaux d'événements Windows

1. Sur l'instance, ouvrez le fichier `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` dans un éditeur de texte.
2. Configurez les paramètres de journaux suivants au besoin et enregistrez vos modifications.

```
{
  "events": [
    {
      "logName": "System",
      "source": "An event source (optional)",
      "level": "Error | Warning | Information",
      "numEntries": 3
    }
  ]
}
```

3. Sous Windows PowerShell, exécutez la commande suivante afin que le système planifie l'exécution du script en tant que tâche planifiée Windows à chaque démarrage de l'instance.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -
Schedule
```

Trois minutes trois ou plus peuvent être nécessaires pour voir les journaux dans la console EC2.

Envoi du message « Windows Is Ready » après un démarrage réussi

Le service EC2Config envoyait le message « Windows est prêt » dans la console EC2 après chaque démarrage. EC2Launch envoie ce message uniquement après le démarrage initial. Pour assurer la rétrocompatibilité avec le service EC2Config, vous pouvez programmer EC2Launch de sorte à envoyer ce message après chaque démarrage. Sur l'instance, ouvrez Windows PowerShell et exécutez la commande suivante. Le système programme le script pour s'exécuter en tant que tâche planifiée Windows.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -
Schedule
```

Historique des versions EC2Launch

Les AMI Windows à partir de Windows Server 2016 incluent un ensemble de scripts Windows PowerShell appelé EC2Launch. EC2Launch effectue des tâches suivantes pendant le démarrage initial de l'instance. Pour plus d'informations sur les versions d'EC2Launch incluses dans les AMI AWS Windows, consultez l'historique des [versions des AWS AMI Windows](#).

Pour télécharger et installer la version la plus récente d'EC2Launch, consultez [Installer la version la plus récente d'EC2Launch](#).

Le tableau suivant décrit les versions publiées d'EC2Launch. Notez que le format de version a changé après la version 1.3.610.

Version	Détails	Date de publication
1,3.2004891	<ul style="list-style-type: none">• Correction d'un problème en raison duquel le paramètre <code>n'HandleUserData</code> était pas réglé <code>false</code> comme prévu.	31 mai 2024

Version	Détails	Date de publication
	<ul style="list-style-type: none">• Ajout d'une option <code>Encrypted</code> de mot de passe à <code>LaunchConfig.json</code> .• <code>Settings UIComportement</code> modifié pour chiffrer le mot de passe spécifié par l'utilisateur par défaut.• Ajouté <code>SetAdminPasswordConfig.ps1</code> pour convertir l'option de <code>Specify</code> mot de passe en option de <code>Encrypted</code> mot de passe dans le fichier de configuration de l'agent.	
1,3.2004617	<ul style="list-style-type: none">• Correction d'une erreur lors du réglage du fond d'écran.	15 janvier 2024

Version	Détails	Date de publication
1,3.2004592	<ul style="list-style-type: none">• Autorisations d'accès mises à jour définies par <code>install.ps1</code> pour <code>%ProgramData%\Amazon\EC2-Windows\Launch</code>.• Accès restreint au dossier/fichier <code>EC2Launch</code> pour lecture-exécution uniquement pour les comptes utilisateur standard.• Modification de l'agent pour arrêter d'attendre l'initialisation du service de métadonnées d'instance (IMDS) si l'IMDS n'est pas activé pour l'instance.• Ajout d'un délai d'attente de cinq minutes lors de l'initialisation de l'IMDS.• Modification de l'agent pour qu'il enregistre la télémétrie dans le journal de la console de l'instance avant le message <code>Windows is Ready</code> plutôt qu'après.• Ajout de la prise en charge du fond d'écran à plusieurs nouveaux types d'instance. <p>Pour plus d'informations sur les autorisations d'accès et les autorisations de compte utilisateur des annuaires <code>EC2Launch</code>, consultez the section called "Structure du répertoire EC2Launch"</p>	2 janvier 2024
1,3.2004491	<ul style="list-style-type: none">• Ajout d'une télémétrie pour surveiller l'utilisation de l'option <code>Spécifier le mot de passe administrateur</code>.	9 novembre 2023
1,3.2004462	<ul style="list-style-type: none">• Ajout d'un vidage après chaque écriture sur la console série.	18 octobre 2023

Version	Détails	Date de publication
1,3.2004438	<ul style="list-style-type: none">• Limite la dévolution des noms de domaine en fonction de l'entrée dans le registre : <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel</code> .• Autorisations <code>UserdataExecution.log</code> limitées à <code>Administrators</code> uniquement.• Des messages d'erreur ont été ajoutés dans le journal des événements Windows en cas d'échec de l'initialisation du journal.	4 octobre 2023
1,3.2004256	<ul style="list-style-type: none">• Valeur <code>EnableSCSIPersistentReservations</code> ajoutée au journal de la console.• Capacité de nouvelle tentative ajoutée pour <code>Get-ConsolePort</code>.	7 juillet 2023
1,3.2004052	<ul style="list-style-type: none">• Correction d'un problème qui survenait lorsqu'aucune clé SSH n'était spécifiée au lancement de l'instance.• Mise à jour pour réessayer de démarrer le service <code>AmazonSSMAgent Windows</code> en cas d'échec.• Mis à jour pour échouer <code>SysprepInstance.ps1</code> si <code>BeforeSysprep.cmd</code> échoue avec un code de sortie différent de zéro.	8 mars 2023
1,3.2003975	<ul style="list-style-type: none">• Correction d'un problème affectant la création de l'AMI Packer où <code>SysprepInstance.ps1</code> renvoie une valeur <code>\$LastErrorCode</code> de 1.	24 décembre 2022

Version	Détails	Date de publication
1,3.2003961	<ul style="list-style-type: none">• Correction d'un problème selon lequel les mots de passe administrateur spécifiés de manière explicite étaient remplacés par un mot de passe aléatoire sur les instances à lancement rapide.• Correction d'un problème selon lequel l'agent SSM ne démarrait pas sur des types d'instances plus petits.• Correction d'un problème selon lequel le journal de la console de l'instance contenait RDPCERTIFICATE-THUMBPRINT : 00000000000000000000000000000000 au lieu d'une valeur d'empreinte numérique valide.	6 décembre 2022
1,3.2003923	<ul style="list-style-type: none">• Corrige la logique de recherche de l'adaptateur réseau lorsque PnPDeviceID est vide.	9 novembre 2022
1,3.2003919	<ul style="list-style-type: none">• Informations mises à jour ConsolePort sur le segment PCI d'accès à l'utilisation.• Correction d'un problème selon lequel la sélection d'une carte réseau est incorrecte après un redémarrage.• Correction de la logique d'expiration start-SSM-Agent.• Correction de la rétrocompatibilité pour l'alias de AdminCredentials la fonction d'envoi.	8 novembre 2022
1,3.2003857	<ul style="list-style-type: none">• Hiérarchise les cartes dotées d'une passerelle par défaut lorsque la carte réseau principale est sélectionnée.• Chiffrement des mots de passe en mémoire étendu.	3 octobre 2022

Version	Détails	Date de publication
1,3.2003824	<ul style="list-style-type: none">• Correction d'une erreur pendant <code>setComputerName</code> .• Ajout d'une logique permettant d'ignorer l'activation de Windows lorsqu'un code de facturation BYOL est détecté.• Ajout du chiffrement des mots de passe en mémoire.• Correction d'une erreur pendant l'initialisation du volume sur <code>m6id.4xlarge</code> .	30 août 2022
1,3.2003691	<ul style="list-style-type: none">• Logique d'attente IMDS mise à jour pour effectuer uniquement des requêtes IMDSv2.• Correction d'un bogue ayant un impact sur l'installation d'eGPU.	21 juin 2022
1,3.2003639	<ul style="list-style-type: none">• Ajout d'une logique d'attente de la carte réseau pour empêcher l'utilisation avant l'initialisation.• Des problèmes mineurs ont été résolus.	10 mai 2022
1,3.2003498	<ul style="list-style-type: none">• Ajout de la télémétrie.• Ajout du raccourci vers l'interface utilisateur des paramètres.• PowerShell Scripts formatés.• Le problème d'arrêt survenant avant la fin du BeforeSysprep fichier <code>.cmd</code> a été résolu.	31 janvier 2022
1,3.2003411	Modification de la logique de génération de mot de passe pour exclure les mots de passe de faible complexité.	4 août 2021
1,3.2003364	Installation mise à jour EgpuManager avec support IMDSv2.	7 juin 2021

Version	Détails	Date de publication
1,3.2003312	<ul style="list-style-type: none"> Ajout de lignes de journal avant et après le paramètre <code>setMonitorAlwaysOn</code> . La version du package AWS Nitro Enclaves a été ajoutée au journal de la console. 	04 mai 2021
1.3.2003284	Modèle d'autorisation amélioré grâce à la mise à jour de l'emplacement pour stocker les données utilisateur vers <code>LocalAppData</code> .	23 mars 2021
1.3.2003236	<ul style="list-style-type: none"> Méthode mise à jour pour définir le mot de passe utilisateur dans <code>Set-AdminAccount</code> et <code>Randomize-LocalAdminPassword</code> . Correction de <code>InitializeDisks</code> pour vérifier si le disque est configuré en lecture seule avant de le définir en écriture. 	11 février 2021
1.3.2003210	Correction de localisation pour <code>install.ps1</code> .	7 janvier 2021
1.3.2003205	Correction de sécurité pour <code>install.ps1</code> pour mettre à jour les autorisations sur le répertoire <code>%ProgramData%AmazonEC2-WindowsLaunchModuleScripts</code> .	28 décembre 2020
1.3.2003189	<code>w32tm resync</code> ajouté après l'ajout des routes.	4 décembre 2020
1.3.2003155	Informations du type d'instance mises à jour.	25 août 2020
1.3.2003150	Ajout de <code>OsCurrentBuild</code> et <code>OsReleaseId</code> à la sortie de la console.	22 avril 2020
1.3.2003040	Correction de la logique de secours IMDS version 1.	7 avril 2020
1.3.2002730	Ajout de la prise en charge d'IMDS V2.	3 mars 2020
1.3.2002240	Des problèmes mineurs ont été résolus.	31 octobre 2019

Version	Détails	Date de publication
1.3.2001660	Problème de connexion automatique résolu pour les utilisateurs sans mot de passe après la première exécution de SysPrep.	2 juillet 2019
1.3.2001360	Des problèmes mineurs ont été résolus.	27 mars 2019
1.3.2001220	Tous les PowerShell scripts sont signés.	28 février 2019
1.3.2001200	Résolution d'un problème lié au InitializeDisks fichier .ps1 selon lequel l'exécution du script sur un nœud d'un cluster Windows Server Failover formatait les disques situés sur des nœuds distants dont la lettre du lecteur correspondait à la lettre du lecteur local.	27 février 2019
1.3.2001160	Correction du problème de papier peint manquant dans Windows 2019.	22 février 2019
1.3.2001040	<ul style="list-style-type: none">• Ajout d'un plugin afin que le moniteur ne s'éteigne jamais pour résoudre les problèmes ACPI.• Édition et version du serveur SQL Server écrites dans la console.	21 janvier 2019
1.3.2000930	Correctif permettant d'ajouter des routes aux métadonnées sur les interfaces réseau Elastic (ENI) activées pour IPv6.	2 janvier 2019
1.3.2000760	<ul style="list-style-type: none">• Ajout d'une configuration par défaut pour RSS et des paramètres de file d'attente de réception pour des périphériques ENA.• Désactivation de la mise en veille prolongée lors de Sysprep	5 décembre 2018

Version	Détails	Date de publication
1.3.2000630	<ul style="list-style-type: none"> • Ajout de la route 169.254.169.253/32 pour le serveur DNS. • Ajout d'un filtre pour le paramétrage de l'utilisateur Admin • Améliorations apportées à la mise en veille prolongée d'instances. • Ajout d'une option de planification d'EC2Launch pour exécution lors de chaque démarrage. 	9 novembre 2018
1.3.2000430.0	<ul style="list-style-type: none"> • Ajout de la route 169.254.169.123/32 au service de temps AMZN. • Ajout de la route 169.254.169.249/32 au service de licence GRID. • Ajout d'un délai d'attente de 25 secondes lors de la tentative de démarrage de Systems Manager. 	19 septembre 2018
1.3.200039.0	<ul style="list-style-type: none"> • Résolution du problème de lettre de lecteur incorrect pour les volumes NVME EBS. • Ajout d'une journalisation supplémentaire pour les versions de pilote NVME. 	15 août 2018
1.3.2000080	Des problèmes mineurs ont été résolus.	
1.3.610	Correction d'un problème lié à la redirection des sorties et des erreurs vers des fichiers à partir de données utilisateur.	
1.3.590	<ul style="list-style-type: none"> • Ajout de types d'instance manquant dans le papier peint. • Résolution d'un problème de mappage de lettre de lecteur et d'installation de disque. 	

Version	Détails	Date de publication
1.3.580	<ul style="list-style-type: none">• Get-Metadata corrigé afin d'utiliser les paramètres de proxy système par défaut pour les demandes web.• Ajout d'un cas particulier pour NVMe dans l'initialisation du disque.• Des problèmes mineurs ont été résolus.	
1.3.550	Ajout d'une option -NoShutdown pour activer Sysprep sans arrêt.	
1.3.540	Des problèmes mineurs ont été résolus.	
1.3.530	Des problèmes mineurs ont été résolus.	
1.3.521	Des problèmes mineurs ont été résolus.	
1.3.0	<ul style="list-style-type: none">• Un problème de longueur hexadécimale a été résolu pour le changement de nom d'ordinateur.• Une éventuelle boucle de redémarrage a été corrigée pour le changement de nom d'ordinateur.• Un problème de configuration du papier peint a été résolu.	
1.2.0	<ul style="list-style-type: none">• Mise à jour permettant d'afficher des informations sur le système d'exploitation installé dans le journal système EC2.• Mise à jour permettant d'afficher EC2Launch et la version de SSM Agent dans le journal système EC2.• Des problèmes mineurs ont été résolus.	

Version	Détails	Date de publication
1.1.2	<ul style="list-style-type: none">• Mise à jour permettant d'afficher les informations du pilote ENA dans le journal système EC2.• Mise à jour permettant d'exclure Hyper-V de la logique des filtres de la carte NIC principale.• AWS KMS Serveur et port ajoutés dans la clé de registre pour l'activation du KMS.• La configuration du papier peint pour plusieurs utilisateurs a été améliorée.• Mise à jour permettant d'effacer les routes du magasin persistant.• Mise à jour permettant de supprimer le z de la zone de disponibilité dans la liste des suffixes DNS.• Mise à jour pour résoudre un problème lié à la balise <run AsLocal System> dans les données utilisateur.	
1.1.1	Première version.	

Configuration d'une instance Windows à l'aide du service EC2Config (ancien)

Note

La documentation EC2Config est fournie à titre de référence historique uniquement. Les versions du système d'exploitation sur lesquelles il s'exécute ne sont plus prises en charge par Microsoft. Nous vous recommandons vivement de passer au dernier service de lancement.

Le service de lancement le plus récent pour Windows Server 2022 est [EC2Launch v2](#), qui remplace EC2Config et EC2Launch.

Les AMI Windows pour les versions de Windows Server antérieures à Windows Server 2016 incluent un service optionnel, le service EC2Config (`EC2Config.exe`). EC2Config est lancé lorsque l'instance démarre et effectue des tâches au moment du démarrage et chaque fois que vous arrêtez ou redémarrez l'instance. EC2Config peut également effectuer des tâches à la demande. Certaines de ces tâches sont automatiquement activées, alors que d'autres doivent être activées manuellement. Bien que facultatif, ce service offre l'accès à des fonctions avancées indisponibles dans d'autres cas. Ce service s'exécute dans le LocalSystem compte.

Note

EC2Launch a remplacé EC2Config sur les AMI Windows pour Windows Server 2016 et 2019. Pour plus d'informations, consultez [Configurer une instance Windows à l'aide d'EC2Launch](#). Le dernier service de lancement pour toutes les versions de Windows Server prises en charge est [EC2Launch v2](#), qui remplace EC2Config et EC2Launch.

EC2Config utilise des fichiers de paramètres pour contrôler son fonctionnement. Vous pouvez mettre à jour ces fichiers de paramètres à l'aide d'un outil graphique ou en modifiant directement les fichiers XML. Les fichiers binaires et les fichiers supplémentaires du service sont stockés dans le répertoire `%ProgramFiles%\Amazon\EC2ConfigService`.

Sommaire

- [Tâches EC2Config](#)
- [Installer la dernière version d'EC2Config](#)
- [Arrêter, redémarrer, supprimer ou désinstaller EC2Config](#)
- [EC2Config et AWS Systems Manager](#)
- [EC2Config et Sysprep](#)
- [Propriétés du service EC2](#)
- [Fichiers de paramètres EC2Config](#)
- [Configurer les paramètres de proxy pour le service EC2Config](#)
- [Historique des versions EC2Config](#)
- [Résoudre les problèmes liés au service EC2Config](#)

Tâches EC2Config

EC2Config exécute des tâches de startup initiales lorsque l'instance est démarrée pour la première fois, puis les désactive. Pour les réexécuter, vous devez les activer explicitement avant d'arrêter l'instance ou en exécutant Sysprep manuellement. Ces tâches se présentent comme suit :

- Définissez un mot de passe chiffré aléatoire pour le nouveau compte d'administrateur.
- Générez et installez le certificat d'hôte utilisé pour la connexion au Bureau à distance.
- Étendez de manière dynamique la partition du système d'exploitation pour inclure l'espace non partitionné.
- Exécutez les données utilisateur spécifiées (et Cloud-Init, s'il est installé). Pour plus d'informations sur la spécification de données utilisateur, consultez [Utiliser les données utilisateur d'instance](#).

EC2Config exécute les tâches suivantes chaque fois que l'instance démarre.

- Modifiez le nom d'hôte pour que celui-ci corresponde à l'adresse IP privée dans la notation hexadécimale (cette tâche est désactivée par défaut et doit être activée pour s'exécuter au démarrage de l'instance).
- Configurez le serveur gestionnaire de clés (AWS KMS), vérifiez l'état de l'activation Windows et activez Windows au besoin.
- Montez tous les volumes Amazon EBS et les volumes de stockage d'instances, et mappez les noms des volumes aux lettres des lecteurs.
- Ecrivez les entrées du journal d'événements sur la console pour faciliter le dépannage (cette tâche est désactivée par défaut et doit être activée pour s'exécuter au démarrage de l'instance).
- Ecrivez sur la console que Windows est prêt.
- Ajoutez un acheminement personnalisé sur la carte réseau principale pour activer les adresses IP suivantes lorsqu'une ou plusieurs cartes réseau sont attachées : 169.254.169.250, 169.254.169.251 et 169.254.169.254. Ces adresses sont utilisées par l'activation de Windows et lorsque vous accédez aux métadonnées de l'instance.

Note

Si le système d'exploitation Windows est configuré pour utiliser IPv4, ces adresses de lien locales IPv4 peuvent être utilisées. Si la pile de protocoles réseau IPv4 est désactivée sur le système d'exploitation Windows et utilise IPv6 à la place, ajoutez

[fd00:ec2::240] à la place de 169.254.169.250 et 169.254.169.251. Ensuite, ajoutez [fd00:ec2::254] à la place de 169.254.169.254.

EC2Config exécute la tâche suivante chaque fois qu'un utilisateur se connecte :

- Affiche les informations du papier peint sur l'arrière-plan du bureau.

Pendant que l'instance s'exécute, vous pouvez demander que EC2Config exécute la tâche suivante à la demande :

- Exécutez Sysprep et arrêtez l'instance afin de créer une AMI à partir de celle-ci. Pour plus d'informations, consultez [Création d'une AMI avec Windows Sysprep](#).

Installer la dernière version d'EC2Config

Par défaut, le service EC2Config est inclus dans les AMI antérieures à Windows Server 2016. Lorsque le service EC2Config est mis à jour, les nouvelles AMI Windows AWS incluent la dernière version du service. Toutefois, vous devez mettre à jour vos propres AMI et instances Windows avec la version la plus récente d'EC2Config.

Note

EC2Launch remplace EC2Config sur les AMI Windows Server 2016 et 2019. Pour plus d'informations, consultez [Configurer une instance Windows à l'aide d'EC2Launch](#). Le dernier service de lancement pour toutes les versions de Windows Server prises en charge est [EC2Launch v2](#), qui remplace EC2Config et EC2Launch.

Pour découvrir comment recevoir des notifications en cas de mise à jour d'EC2Config, consultez [S'abonner aux notifications du service EC2Config](#). Pour plus d'informations sur les modifications apportées à chaque version, consultez le document [Historique des versions EC2Config](#).

Avant de commencer

- Vérifiez que vous disposez de .NET Framework 3.5 SP1 ou supérieur.
- Par défaut, la configuration remplace vos fichiers de paramètres par les fichiers de paramètres par défaut pendant l'installation et redémarre le service EC2Config une fois l'installation terminée.

Si vous avez modifié les paramètres de service EC2Config, copiez le fichier `config.xml` depuis le répertoire `%Program Files%\Amazon\Ec2ConfigService\Settings`. Une fois que vous avez mis à jour le service EC2Config, vous pouvez restaurer ce fichier pour conserver les modifications de configuration.

- Si votre version d'EC2Config est antérieure à la version 2.1.19 et que vous installez la version 2.2.12 ou une version antérieure, vous devez d'abord installer la version 2.1.19. Pour installer la version 2.1.19, téléchargez le fichier [EC2Install_2.1.19.zip](#), décompressez-le et exécutez `EC2Install.exe`.

Note

Si votre version d'EC2Config est antérieure à la version 2.1.19 et que vous installez la version 2.3.313 ou suivante, vous pouvez l'installer directement sans d'abord installer la version 2.1.19.

Vérifier la version d'EC2Config

Utilisez la procédure suivante pour vérifier la version d'EC2Config installée sur vos instances.

Pour vérifier la version installée d'EC2Config

1. Lancez une instance depuis votre AMI et connectez-vous à celle-ci.
2. Dans le Panneau de configuration, sélectionnez Programmes et fonctionnalités.
3. Dans la liste des programmes installés, recherchez `Ec2ConfigService`. Son numéro de version s'affiche dans la colonne Version.

Mise à jour d'EC2Config

Utilisez la procédure suivante pour télécharger et installer manuellement la version la plus récente d'EC2Config sur vos instances.

Pour télécharger et installer la version la plus récente d'EC2Config

1. Téléchargez et décompressez le [programme d'installation d'EC2Config](#).
2. Exécutez `EC2Install.exe`. Pour obtenir une liste complète des options, exécutez `EC2Install` avec l'option `/?`. Par défaut, la configuration affiche les invites. Pour exécuter la commande sans invites, utilisez l'option `/quiet`.

⚠ Important

Pour conserver les paramètres personnalisés du fichier `config.xml` que vous avez enregistrés, exécutez `EC2Install` avec l'option `/norestart`, restaurez vos paramètres, puis redémarrez le service `EC2Config` manuellement.

3. Si vous exécutez `EC2Config` version 4.0 ou ultérieure, vous devez redémarrer `SSM Agent` sur l'instance depuis le composant logiciel enfichable `Microsoft Services`.

ℹ Note

Les informations de version mises à jour d'`EC2Config` n'apparaîtront pas dans le journal système de l'instance ou dans la vérification `Trusted Advisor` tant que vous n'aurez pas réinitialisé ou arrêté et démarré votre instance.

Pour télécharger et installer la dernière version d'`EC2Config` à l'aide de `PowerShell`

Pour télécharger, décompresser et installer la dernière version d'`EC2Config` à l'aide de `PowerShell`, exécutez les commandes suivantes depuis une fenêtre : `PowerShell`

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.Namespace($ExtractPath).CopyHere($ExtractFiles)
Start-Process $ExtractPath
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

ℹ Note

Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez `Windows Server 2016` ou une version antérieure, il est possible que le protocole `TLS 1.2` doive être activé sur votre `PowerShell` terminal. Vous pouvez activer le protocole `TLS 1.2` pour la `PowerShell` session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Vérifiez l'installation en vérifiant que le répertoire C:\Program Files\Amazon\ contient le répertoire Ec2ConfigService.

Arrêter, redémarrer, supprimer ou désinstaller EC2Config

Vous pouvez gérer le service EC2Config comme tout autre service.

Pour appliquer les paramètres mis à jour dans votre instance, vous pouvez arrêter et redémarrer le service. Si vous installez manuellement EC2Config, vous devez d'abord arrêter le service.

Pour arrêter le service EC2Config

1. Lancez et connectez-vous à votre instance Windows.
2. Sur le menu Démarrer, pointez la souris vers Outils d'administration et cliquez sur Services.
3. Dans la liste des services, cliquez avec le bouton droit sur EC2Config et sélectionnez Arrêter.

Pour redémarrer le service EC2Config

1. Lancez et connectez-vous à votre instance Windows.
2. Sur le menu Démarrer, pointez la souris vers Outils d'administration et cliquez sur Services.
3. Dans la liste des services, cliquez avec le bouton droit sur EC2Config et sélectionnez Redémarrer.

Si vous n'avez pas besoin de mettre à jour les paramètres de configuration, créez votre propre AMI ou utilisez AWS Systems Manager. Vous pouvez supprimer et désinstaller le service. La suppression d'un service entraîne celle de sa sous-clé du registre. La désinstallation d'un service entraîne la suppression des fichiers, de la sous-clé du registre et de tous les raccourcis vers le service.

Pour supprimer le service EC2Config

1. Démarrez une fenêtre d'invite de commande.
2. Exécutez la commande suivante :

`sc delete ec2config`

Pour désinstaller EC2Config

1. Lancez et connectez-vous à votre instance Windows.
2. Dans le menu Démarrer, cliquez sur Panneau de configuration.
3. Double-cliquez sur Programmes et fonctionnalités.
4. Dans la liste des programmes, sélectionnez EC2 ConfigService, puis cliquez sur Désinstaller.

EC2Config et AWS Systems Manager

Le service EC2Config traite les demandes Systems Manager sur les instances créées à partir d'AMI pour des versions de Windows Server antérieures à Windows Server 2016 publiées avant novembre 2016.

Les instances créées à partir d'AMI pour des versions de Windows Server antérieures à Windows Server 2016 qui ont publiées avant novembre 2016 incluent le service EC2Config et SSM Agent. EC2Config exécute toutes les tâches décrites précédemment, et SSM Agent traite les requêtes des fonctionnalités Systems Manager telles que Exécuter la commande et State Manager.

Vous pouvez utiliser la fonctionnalité Exécuter la commande pour mettre à niveau les instances existantes et utiliser la dernière version du service EC2Config et de SSM Agent. Pour plus d'informations, consultez [Update SSM Agent by using Run Command](#) dans le Guide de l'utilisateur AWS Systems Manager .

EC2Config et Sysprep

Le service EC2Config exécute Sysprep, un outil Microsoft qui vous permet de créer une AMI Windows personnalisée qui peut être réutilisée. Quand EC2Config appelle Sysprep, il utilise les fichiers présents dans %ProgramFiles%\Amazon\EC2ConfigService\Settings pour déterminer les opérations à effectuer. Vous pouvez modifier ces fichiers indirectement à l'aide de la boîte de dialogue EC2 Service Properties (Propriétés du service EC2), ou directement à l'aide d'un éditeur XML ou d'un éditeur de texte. Toutefois, certains paramètres avancés ne sont pas disponibles dans la boîte de dialogue Propriétés du service Ec2 ; vous devez donc modifier ces entrées directement.

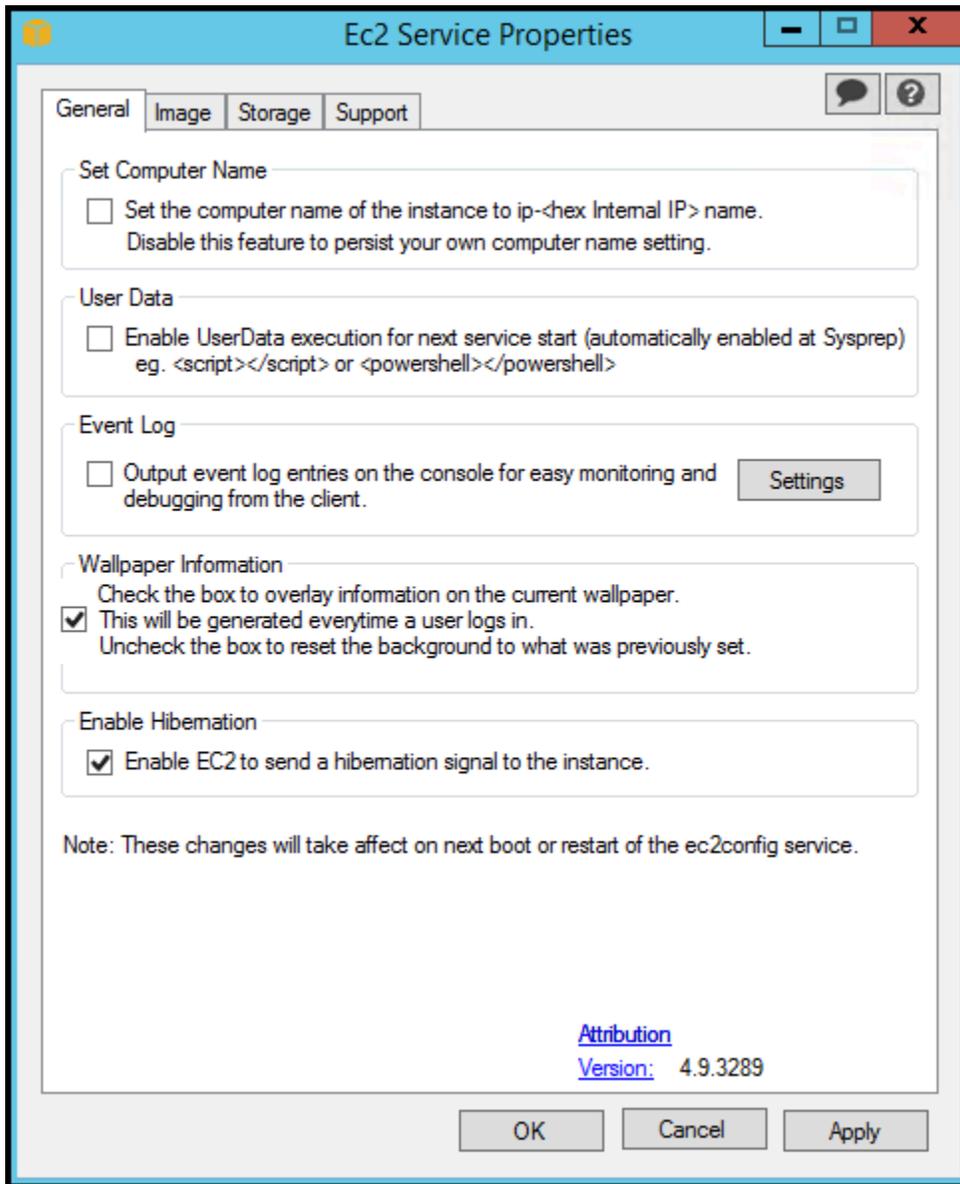
Si vous créez une AMI directement dans une instance après avoir mis à jour ses paramètres, ceux-ci sont appliqués à n'importe quelle instance lancée dans la nouvelle AMI. Pour plus d'informations sur la création d'une AMI, consultez [Création d'une AMI basée sur Amazon EBS](#).

Propriétés du service EC2

La procédure suivante décrit comment utiliser le service la boîte de dialogue EC2 Service Properties (Propriétés du service EC2) pour activer ou désactiver les paramètres.

Pour modifier les paramètres à l'aide de la boîte de dialogue Ec2 Service Properties (Propriétés du service EC2)

1. Lancez et connectez-vous à votre instance Windows.
2. Dans le menu Démarrer, cliquez sur Tous les programmes, puis sur ConfigServiceParamètres EC2.



3. Sur l'onglet General (Général) de la boîte de dialogue EC2 Service Properties (Propriétés du service EC2), vous pouvez activer ou désactiver les paramètres suivants.

Set Computer Name (Définir le nom de l'ordinateur)

Si ce paramètre est activé (il est désactivé par défaut), le nom d'hôte est comparé à l'adresse IP interne actuelle à chaque démarrage. Si le nom d'hôte et l'adresse IP interne ne correspondent pas, le nom d'hôte est réinitialisé pour contenir l'adresse IP interne, puis le système redémarre pour récupérer le nouveau nom d'hôte. Pour définir votre propre nom d'hôte ou pour empêcher que votre nom d'hôte existant soit modifié, n'activez pas ce paramètre.

User Data (Données utilisateur)

L'exécution des données utilisateur vous permet de spécifier des scripts dans les métadonnées de l'instance. Par défaut, ces scripts sont exécutés lors du lancement initial. Vous pouvez également les configurer pour les exécuter la prochaine fois que vous réamorcez ou démarrez l'instance, ou chaque fois que vous réamorcez ou démarrez l'instance.

Si vous avez un script volumineux, nous vous recommandons d'utiliser les données utilisateur pour télécharger le script, puis de l'exécuter.

Pour plus d'informations, consultez [Exécution de données utilisateur](#).

Event Log

Utilisez ce paramètre pour afficher les entrées du journal d'événements sur la console pendant le démarrage afin de simplifier la surveillance et le débogage.

Cliquez sur Settings (Paramètres) pour spécifier des filtres pour les entrées du journal envoyées à la console. Le filtre par défaut envoie les trois entrées d'erreurs les plus récentes du journal d'événements du système vers la console.

Wallpaper Information (Informations sur le papier peint)

Utilisez ce paramètre pour afficher les informations système sur l'arrière-plan du bureau. L'exemple suivant présente les informations affichées sur l'arrière-plan du bureau.

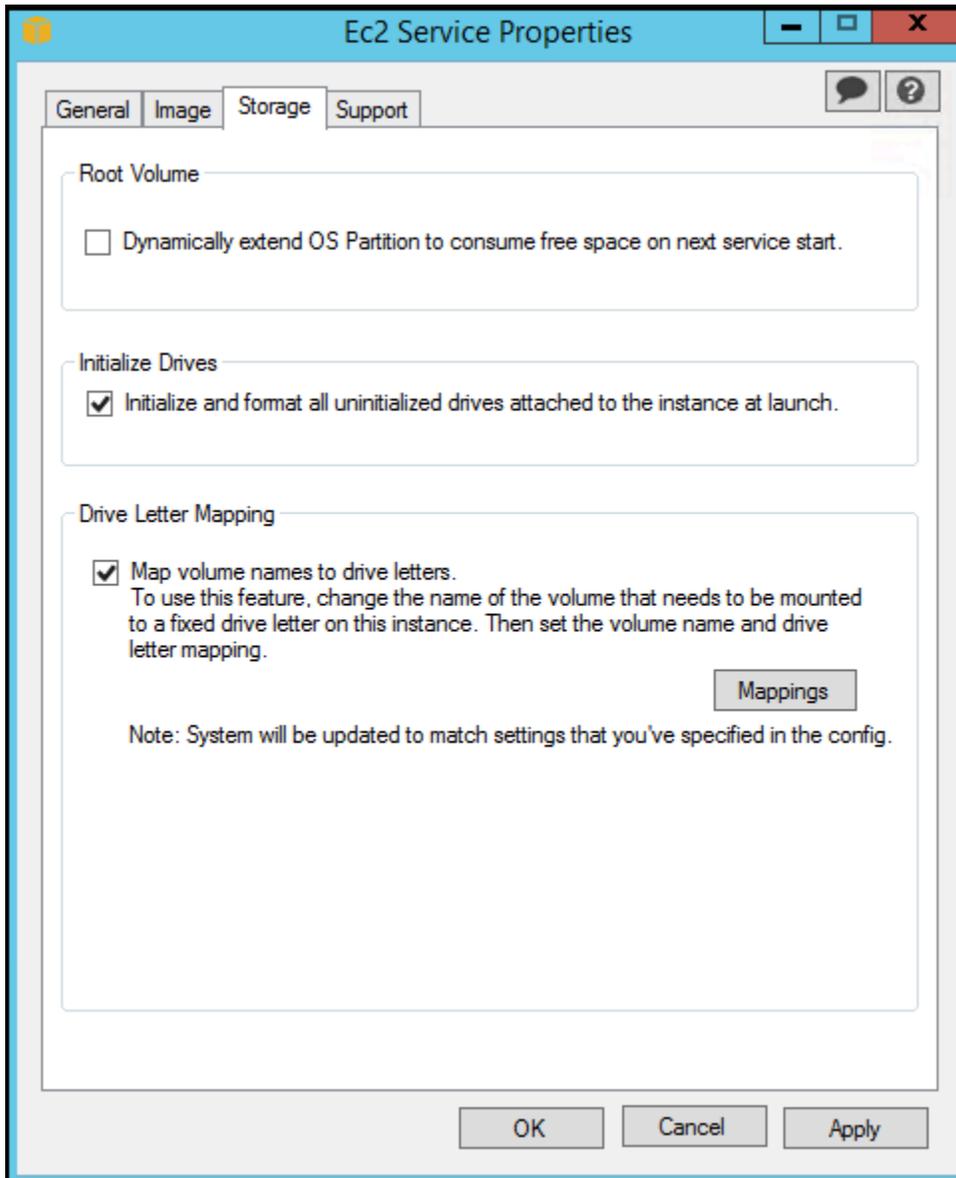
```
Hostname      : WIN-U0RFOJCTPUU
Instance ID   : i-d583f76a
Public IP Address : 54.208.43.227
Private IP Address : 172.31.42.195
Availability Zone : us-east-1b
Instance Size  : t2.micro
Architecture  : AMD64
```

Les informations affichées à l'arrière-plan du bureau sont contrôlées par le fichier de paramètres `EC2ConfigService\Settings\WallpaperSettings.xml`.

Enable Hibernation (Activer la mise en veille prolongée)

Utilisez ce paramètre pour autoriser EC2 à demander au système d'exploitation d'effectuer la mise en veille prolongée.

4. Cliquez sur l'onglet Storage (Stockage). Vous pouvez activer ou désactiver les paramètres suivants.



Root Volume (Volume racine)

Ce paramètre étend de manière dynamique le disque 0/volume 0 pour inclure l'espace non partitionné. Cela peut être utile lorsque l'instance est démarrée à partir d'un volume du périphérique racine doté d'une taille personnalisée.

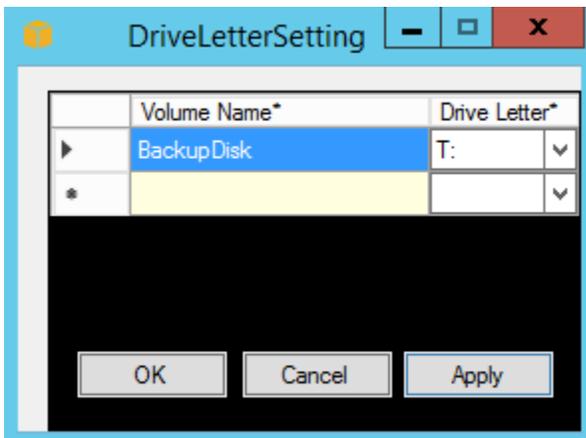
Initialize Drives (Initialiser les lecteurs)

Ce paramètre formate et monte tous les volumes attachés à l'instance au démarrage.

Drive Letter Mapping (Mappage de lettres de lecteur)

Le système mappe les volumes attachés à une instance aux lettres des lecteurs. Pour les volumes Amazon EBS, l'action par défaut consiste à attribuer les lettres de lecteurs de D: à Z:. Par exemple, les volumes de stockage, la valeur par défaut dépend du pilote. AWS Les pilotes PV et Citrix PV attribuent aux volumes de stockage des instances des lettres de lecteur allant de Z : à A :. Les pilotes Red Hat attribuent les lettres de lecteurs de volumes de stockage d'instances allant de D: à A:.

Pour choisir les lettres de lecteurs de vos volumes, cliquez sur Mappings (Mappages). Dans la boîte de dialogue de DriveLetterconfiguration, spécifiez les valeurs du nom du volume et de la lettre du lecteur pour chaque volume, cliquez sur Appliquer, puis sur OK. Nous vous recommandons de sélectionner les lettres de lecteurs qui permettent d'éviter les conflits avec es lettres de lecteurs susceptibles d'être utilisées, comme celles du milieu de l'alphabet.



Après avoir spécifié un mappage de lettres de lecteurs et attaché un volume avec la même étiquette que l'un des noms de volumes que vous avez spécifiés, EC2Config attribue automatiquement à ce volume la lettre de lecteur que vous avez spécifiée. En revanche, le mappage de lettre de lecteur échoue si celle-ci est déjà utilisée. Notez que EC2Config ne modifie pas les lettres de lecteurs des volumes déjà montés lors de la spécification du mappage de lettre de lecteur.

5. Pour enregistrer vos paramètres et continuer de les utiliser ultérieurement, cliquez sur OK pour fermer la boîte de dialogue EC2 Service Properties (Propriétés du service EC2). Si vous avez terminé de personnaliser votre instance et que vous souhaitez créer une AMI à partir de cette instance, consultez [Création d'une AMI avec Windows Sysprep](#).

Fichiers de paramètres EC2Config

Les fichiers de paramètres contrôlent le fonctionnement du service EC2Config. Ces fichiers se trouvent dans le répertoire `C:\Program Files\Amazon\Ec2ConfigService\Settings` :

- `ActivationSettings.xml`—Contrôle l'activation du produit à l'aide d'un serveur gestionnaire de clés (AWS KMS).
- `AWS.EC2.Windows.CloudWatch.json`—Contrôle les compteurs de performance auxquels envoyer CloudWatch et les journaux à envoyer à CloudWatch Logs.
- `BundleConfig.xml` : contrôle la manière dont EC2Config prépare une instance basée sur le stockage d'instances pour la création d'AMI.
- `Config.xml` — Contrôle les paramètres principaux.
- `DriveLetterConfig.xml` — Contrôle les mappages de lettres de lecteurs.
- `EventLogConfig.xml` — Contrôle les informations de journaux d'événements affichés sur la console au démarrage de l'instance.
- `WallpaperSettings.xml` — Contrôle les informations affichées sur l'arrière-plan du bureau.

ActivationSettings.xml

Ce fichier contient les paramètres qui contrôlent l'activation du produit. Au démarrage de Windows, le service EC2Config vérifie si Windows est déjà activé. Si Windows n'est pas le cas, il tente de l'activer en recherchant le serveur AWS KMS spécifié.

- `SetAutodiscover`—Indique si un AWS KMS doit être détecté automatiquement.
- `TargetKMSServer`—Enregistre l'adresse IP privée d'un AWS KMS. Le AWS KMS doit être situé dans la même région que votre instance.
- `DiscoverFromZone`—Découvre le AWS KMS serveur depuis la zone DNS spécifiée.
- `ReadFromUserData`—Récupère le AWS KMS serveur depuis. `UserData`
- `LegacySearchZones`—Découvre le AWS KMS serveur depuis la zone DNS spécifiée.
- `DoActivate` — Fait des tentatives d'activation à l'aide des paramètres spécifiés dans la section. Cette valeur peut être `true` ou `false`.
- `LogResultToConsole` — Affiche le résultat sur la console.

BundleConfig.xml

Ce fichier contient les paramètres qui contrôlent la manière dont EC2Config prépare une instance pour la création de l'AMI.

- `AutoSysprep` — Indique si Sysprep doit être utilisé automatiquement. Modifiez la valeur à `Yes` pour utiliser Sysprep.
- `SetRDPCertificate` — Définit un certificat autosigné sur le serveur des services Bureau à distance. Cela vous permet d'utiliser en toute sécurité le protocole RDP dans les instances. Modifiez la valeur à `Yes` si les nouvelles instances doivent avoir le certificat.

Ce paramètre n'est pas utilisé pour les instances dont les versions du système d'exploitation sont antérieures à Windows Server 2016, car elles peuvent générer leurs propres certificats.

- `SetPasswordAfterSysprep` — Définit un mot de passe aléatoire sur une instance lancée récemment, chiffre celui-ci avec la clé de lancement de l'utilisateur et sort le mot de passe chiffré sur la console. Modifiez la valeur de ce paramètre à `No` si les nouvelles instances ne doivent pas être définies sur un mot de passe chiffré aléatoire.

Config.xml

Plug-ins (Compléments)

- `Ec2SetPassword` — Génère un mot de passe chiffré chaque fois que vous lancez une instance. Par défaut cette fonction est désactivée après le premier lancement afin que les redémarrages de cette instance ne modifient pas un mot de passe défini par l'utilisateur. Modifiez ce paramètre à `Enabled` pour continuer de générer des mots de passe chaque fois que vous lancez une instance.

Ce paramètre est important si vous planifiez de créer une AMI à partir de votre instance.

- `Ec2SetComputerName` — Définit le nom d'hôte de l'instance sur un nom unique basé sur l'adresse IP de l'instance et redémarre l'instance. Pour définir votre propre nom d'hôte ou pour empêcher que votre nom d'hôte existant soit modifié, désactivez ce paramètre.
- `Ec2InitializeDrives` — Initialise et formate tous les volumes au démarrage. Cette caractéristique est activée par défaut.
- `Ec2EventLog` — Affiche les entrées du journal des événements sur la console. Par défaut, les trois entrées d'erreurs les plus récentes du journal d'événements du système sont affichées. Pour spécifier les entrées du journal des événements à afficher, modifiez le fichier `EventLogConfig.xml` situé dans le répertoire `EC2ConfigService\Settings`. Pour plus

d'informations sur les paramètres de ce fichier, consultez [Eventlog Key](#) dans la bibliothèque MSDN.

- `Ec2ConfigureRDP` — Configure un certificat autosigné sur l'instance, afin que les utilisateurs puissent accéder en toute sécurité à l'instance à l'aide des services Bureau à distance. Ce paramètre n'est pas utilisé pour les instances dont les versions du système d'exploitation sont antérieures à Windows Server 2016, car elles peuvent générer leurs propres certificats.
- `Ec2OutputRDPcert` — Affiche les informations du certificat des services Bureau à distance sur la console afin que les utilisateurs puissent les vérifier auprès de l'empreinte numérique.
- `Ec2SetDriveLetter` — Définit les lettres de lecteurs des volumes montés, sur la base des paramètres définis par l'utilisateur. Par défaut, lorsqu'un volume Amazon EBS est attaché à une instance, il peut être monté à l'aide de la lettre de lecteur sur l'instance. Pour spécifier vos mappages de lettres de lecteurs, modifiez le fichier `DriveLetterConfig.xml` situé dans le répertoire `EC2ConfigService\Settings`.
- `Ec2WindowsActivate` — Le plug-in gère l'activation de Windows. Il vérifie si Windows est activé. Dans le cas contraire, il met à jour les paramètres du AWS KMS client, puis active Windows.

Pour modifier les AWS KMS paramètres, modifiez le `ActivationSettings.xml` fichier situé dans le `EC2ConfigService\Settings` répertoire.

- `Ec2DynamicBootVolumeSize` — Étend le disque 0/volume 0 pour inclure l'espace non partitionné.
- `Ec2HandleUserData` — Crée et exécute les scripts créés par l'utilisateur au premier lancement d'une instance une fois Sysprep exécuté. Les commandes encapsulées dans des balises de script sont enregistrées dans un fichier batch, et les commandes encapsulées dans des PowerShell balises sont enregistrées dans un fichier .ps1 (correspond à la case à cocher Données utilisateur de la boîte de dialogue Propriétés du service Ec2).
- `Ec2ElasticGpuSetup` — Installe le package logiciel GPU Elastic si l'instance est associée à un GPU Elastic.
- `Ec2FeatureLogging` — Envoie à la console l'état d'installation de la fonction Windows et du service correspondant. Pris en charge uniquement pour la fonction Microsoft Hyper-V et le service correspondant vmms.

Paramètres globaux

- `ManageShutdown` : vérifie que les instances lancées depuis les AMI basées sur le stockage d'instances ne sont pas résiliées pendant l'exécution de Sysprep.

- `SetDnsSuffixList` — Définit le suffixe DNS de la carte réseau d'Amazon EC2. Cela permet la résolution DNS des serveurs s'exécutant dans Amazon EC2 sans fournir le nom de domaine complet.

Note

Cela ajoute une recherche de suffixe DNS pour le domaine suivant et configure d'autres suffixes standard. Pour plus d'informations sur la façon dont les agents de lancement définissent les suffixes DNS, consultez [Configurer le suffixe DNS pour les agents de lancement Windows](#)

```
region.ec2-utilities.amazonaws.com
```

- `WaitForMetaDataAvailable` — Vérifie que le service EC2Config attend que les métadonnées soient accessibles et que le réseau soit disponible avant de poursuivre le démarrage. Cela vérifie que EC2Config peut obtenir des informations auprès des métadonnées de l'activation et d'autres plugins.
- `ShouldAddRoutes` — Ajoute une route personnalisée sur la carte réseau principale pour activer les adresses IP suivantes lorsque plusieurs cartes réseau sont attachées : 169.254.169.250, 169.254.169.251 et 169.254.169.254. Ces adresses sont utilisées par l'activation de Windows et lorsque vous accédez aux métadonnées de l'instance.
- `RemoveCredentialsfromSysprepOnStartup` — Supprime le mot de passe administrateur du fichier `Sysprep.xml` au démarrage suivant du service. Pour vous assurer que le mot de passe persiste, modifiez le paramètre.

DriveLetterConfig.xml

Ce fichier contient les paramètres qui contrôlent les mappages de lettres de lecteurs. Par défaut, un volume peut être mappé à n'importe quelle lettre de lecteur disponible. Vous pouvez monter un volume sur une lettre de lecteur spécifique comme indiqué ci-après.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
```

```
<Mapping>
  <VolumeName></VolumeName>
  <DriveLetter></DriveLetter>
</Mapping>
</DriveLetterMapping>
```

- `VolumeName` — Étiquette du volume. Par exemple, *My Volume*. Pour spécifier un mappage pour un volume de stockage d'instance, utilisez l'étiquette `Temporary Storage X`, où X est un chiffre de 0 à 25.
- `DriveLetter` — Lettre du lecteur. Par exemple, *M:*. Le mappage de la lettre du lecteur échoue si celle-ci est déjà utilisée.

EventLogConfig.xml

Ce fichier contient les paramètres qui contrôlent les informations de journaux d'événements affichés sur la console au démarrage de l'instance. Par défaut, les trois entrées d'erreurs les plus récentes du journal d'événements du système sont affichées.

- `Category` — Clé du journal des événements à surveiller.
- `ErrorType` — Type d'événement (par exemple, `Error`, `Warning`, `Information`.)
- `NumEntries` — Nombre d'événements stockés pour cette catégorie.
- `LastMessageTime` — Pour empêcher que le même message soit envoyé de manière répétée, le service met à jour cette valeur chaque fois qu'il envoie un message.
- `AppName` — Source de l'événement ou application ayant enregistré l'événement.

WallpaperSettings.xml

Ce fichier contient les paramètres qui contrôlent les informations affichées sur l'arrière-plan du bureau. Les informations suivantes sont affichées par défaut.

- `Hostname` — Affiche le nom de l'ordinateur.
- `Instance ID` — Affiche l'ID de l'instance.
- `Public IP Address` — Affiche l'adresse IP publique de l'instance.
- `Private IP Address` — Affiche l'adresse IP privée de l'instance.
- `Availability Zone` — Affiche la zone de disponibilité dans laquelle l'instance s'exécute.
- `Instance Size` — Affiche le type de l'instance.

- **Architecture** — Affiche le paramètre de la variable d'environnement `PROCESSOR_ARCHITECTURE`.

Vous pouvez supprimer toutes les informations affichées par défaut en supprimant leurs entrées. Vous pouvez ajouter les métadonnées de l'instance à afficher comme suit.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifiant>meta-data/path</identifiant>
</WallpaperInformation>
```

Vous pouvez ajouter les variables d'environnement du système à afficher comme suit.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifiant>variable-name</identifiant>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Ce fichier contient des paramètres qui contrôlent la façon dont EC2Config initialise les disques.

Par défaut, EC2Config initialise les disques qui n'ont pas été mis en ligne avec le système d'exploitation. Vous pouvez personnaliser le plugin comme suit.

```
<InitializeDrivesSettings>
  <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Utilisez un groupe de paramètres pour spécifier comment vous souhaitez initialiser les disques:

FormatWithGARNITURE

Active la commande TRIM lors du formatage des disques. Une fois qu'un disque a été formaté et initialisé, le système restaure la configuration TRIM.

A partir d'EC2Config version 3.18, la commande TRIM est désactivée pendant l'opération de formatage de disque par défaut. Cela améliore les délais de formatage. Utilisez ce paramètre

pour activer la commande TRIM pendant l'opération de formatage de disque pour EC2Config version 3.18 ou ultérieure.

FormatWithoutGARNITURE

Désactive la commande TRIM lors du formatage des disques et améliore les délais de formatage sous Windows. Une fois qu'un disque a été formaté et initialisé, le système restaure la configuration TRIM.

DisableInitializeDisques

Désactive le formatage des nouveaux disques. Utilisez-le pour initialiser les disques manuellement.

Configurer les paramètres de proxy pour le service EC2Config

Vous pouvez configurer le service EC2Config pour communiquer via un proxy en utilisant l'une des méthodes suivantes : le AWS SDK pour .NETsystem.net, l'élément ou Microsoft Group Policy et Internet Explorer. L'utilisation du AWS SDK pour .NET est la méthode préférée, car vous pouvez spécifier des informations de connexion.

Méthodes

- [Configurez les paramètres du proxy à l'aide du AWS SDK for .NET \(préférée\)](#)
- [Configurer les paramètres de proxy à l'aide de l'élément system.net](#)
- [Configurer les paramètres de proxy à l'aide de la politique de groupe Microsoft et de Microsoft Internet Explorer](#)

Configurez les paramètres du proxy à l'aide du AWS SDK for .NET (préférée)

Vous pouvez configurer les paramètres proxy du service EC2Config en spécifiant l'élément proxy dans le fichier `Ec2Config.exe.config`. Pour plus d'informations, consultez [la section Référence des fichiers de configuration pour le AWS SDK for .NET](#).

Pour spécifier l'élément proxy dans le fichier `Ec2Config.exe.config`

1. Modifiez le fichier `Ec2Config.exe.config` sur une instance dans laquelle vous souhaitez que le service EC2Config communique via un proxy. Par défaut, le fichier se trouve dans le répertoire suivant : `%ProgramFiles%\Amazon\Ec2ConfigService`.

2. Ajoutez l'élément `aws` suivant aux `configSections`. Ne l'ajoutez pas à des `sectionGroups` existants.

Pour EC2Config version 3.17 ou précédente

```
<configSections>
  <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
</configSections>
```

Pour EC2Config version 3.18 ou ultérieure

```
<configSections>
  <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
</configSections>
```

3. Ajoutez l'élément `aws` suivant au fichier `Ec2Config.exe.config`.

```
<aws>
  <proxy
    host="string value"
    port="string value"
    username="string value"
    password="string value" />
</aws>
```

4. Enregistrez vos modifications.

Configurer les paramètres de proxy à l'aide de l'élément `system.net`

Vous pouvez spécifier les paramètres proxy dans un élément `system.net` dans le fichier `Ec2Config.exe.config`. Pour plus d'informations, consultez [defaultProxy Element \(Network Settings\)](#) sur MSDN.

Pour spécifier l'élément `system.net` dans le fichier `Ec2Config.exe.config`

1. Modifiez le fichier `Ec2Config.exe.config` sur une instance dans laquelle vous souhaitez que le service EC2Config communique via un proxy. Par défaut, le fichier se trouve dans le répertoire suivant : `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Ajoutez une entrée `defaultProxy` à `system.net`. Pour plus d'informations, consultez [defaultProxy Element \(Network Settings\)](#) sur MSDN.

Par exemple, la configuration suivante achemine tout le trafic pour utiliser le proxy qui est actuellement configuré pour Internet Explorer, à l'exception des métadonnées et du trafic de licence qui contournent le proxy.

```
<defaultProxy>
  <proxy usesystemdefault="true" />
  <bypasslist>
    <add address="169.254.169.250" />
    <add address="169.254.169.251" />
    <add address="169.254.169.254" />
    <add address="[fd00:ec2::250]" />
    <add address="[fd00:ec2::254]" />
  </bypasslist>
</defaultProxy>
```

3. Enregistrez vos modifications.

Configurer les paramètres de proxy à l'aide de la politique de groupe Microsoft et de Microsoft Internet Explorer

Le service EC2Config s'exécute avec le compte utilisateur du système local. Vous pouvez spécifier des paramètres proxy à l'échelle de l'instance pour ce compte dans Internet Explorer après avoir modifié les paramètres de la politique de groupe sur l'instance.

Pour configurer les paramètres proxy à l'aide de la politique de groupe et d'Internet Explorer

1. Sur une instance dans laquelle vous souhaitez que le service EC2Config communique via un proxy, ouvrez une invite de commande en tant qu'administrateur, tapez **gpedit.msc** et appuyez sur Entrée.
2. Dans l'Editeur de stratégie de groupe locale, sous Stratégie Ordinateur local, choisissez Configuration ordinateur, Modèles d'administration, Composants Windows, Internet Explorer.
3. Dans le volet droit, choisissez Paramètres machine du serveur proxy (plutôt que les paramètres individualisés), puis Modifier les paramètres de la stratégie.
4. Choisissez Activée, puis Appliquer.
5. Ouvrez Internet Explorer, puis cliquez sur le bouton Outils.
6. Choisissez Options Internet, puis choisissez l'onglet Connexions.
7. Choisissez Paramètres réseau.

8. Sous Serveur proxy, choisissez l'option Utiliser un serveur proxy pour le réseau local.
9. Spécifiez l'adresse et les informations sur le port, puis choisissez OK.

Historique des versions EC2Config

Les AMI Windows antérieures à Windows Server 2016 incluent un service facultatif appelé le service Config (EC2Config.exeEC2). EC2Config est lancé lorsque l'instance démarre et effectue des tâches au moment du démarrage et chaque fois que vous arrêtez ou redémarrez l'instance.

Vous pouvez recevoir des notifications en cas de publication de nouvelles versions du service EC2Config. Pour plus d'informations, consultez [S'abonner aux notifications du service EC2Config](#).

Le tableau suivant décrit les versions publiées d'EC2Config. Pour plus d'informations sur les mises à jour de SSM Agent, consultez les [Systems Manager SSM Agent Release Notes](#).

Version	Détails	Date de publication
4,9,5554	<ul style="list-style-type: none"> • Limite la dévolution des noms de domaine en fonction de l'entrée dans le registre : HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel . • Nouvelle version de l'Agent SSM 3.2.1630.0 . 	4 octobre 2023
4,9,5467	<ul style="list-style-type: none"> • Ajout d'une fonctionnalité de nouvelle tentative pour découvrir le port de console. • Nouvelle version de l'Agent SSM 3.1.2282.0 . 	1er août 2023
4,9,5288	<ul style="list-style-type: none"> • Mise à jour du kit SDK Core AWS vers la version 3.7.103.23 . • Correction du problème pour lequel le document SSM AWS-UpdateEC2Config ne mettait pas à jour EC2Config sur les instances activées uniquement avec IMDSv2. 	8 mars 2023

Version	Détails	Date de publication
	<ul style="list-style-type: none"> Nouvelle version de l'Agent SSM 3.1.2144.0 . 	
4,9,5231	<ul style="list-style-type: none"> Nouvelle version de SSM Agent 3.1.1927.0. 	14 février 2023
4,9,5103	<ul style="list-style-type: none"> Correction d'un problème d'identification incorrecte des volumes éphémères sur les familles d'instances r5d et i4i. Nouvelle version de SSM Agent 3.1.1856.0. 	5 décembre 2022
4,9,5064	<ul style="list-style-type: none"> Mise à jour pour utiliser les informations du segment PCI pour sélectionner le port de la console. PowerShell Scripts signés et en-têtes de copyright ajoutés. Correction de la logique de sélection de l'adaptateur réseau principal. Nouvelle version de SSM Agent 3.1.1732.0. 	16 novembre 2022
4,9,4588	<ul style="list-style-type: none"> Logique d'attente IMDS mise à jour pour effectuer uniquement des requêtes IMDSv2. Ajout de la bibliothèque partagée de l'agent de lancement libec2launch.dll. Nouvelle version de SSM Agent 3.1.1188.0. 	31 mai 2022
4,9,4556	<ul style="list-style-type: none"> Ajout d'une logique d'attente pour garantir l'initialisation complète de la carte réseau avant utilisation. La nouvelle version de Log4Net 2.0.14.0 reprend le correctif de sécurité. La nouvelle version de SSM Agent 3.1.1045.0 détecte le correctif de sécurité. 	1 mars 2022

Version	Détails	Date de publication
4,9,4536	<ul style="list-style-type: none">• Correction d'un incident des données utilisateur lorsque le dossier Temp est manquant.• Nouvelle version de SSM Agent (3.1.804.0)	31 janvier 2022
4,9,4508	<ul style="list-style-type: none">• Correction du problème pour calculer correctement le chemin du script diskpart.• Nouvelle version de SSM Agent (3.1.338.0)	6 octobre 2021
4,9,4500	<ul style="list-style-type: none">• Mise à jour de Install-EgpuManagerConfig avec prise en charge d'IMDS v2.• Mise à jour des liens Web pour utiliser https.• Nouvelle version de SSM Agent (3.1.282.0)	7 septembre 2021
4,9,4419	<ul style="list-style-type: none">• Correction de la logique de secours IMDS version 1.• Mise à jour de toute utilisation du répertoire temporaire Windows vers le répertoire temporaire EC2Config• Nouvelle version de SSM Agent 3.0.1124.0	2 juin 2021
4.9.4381	<ul style="list-style-type: none">• Ajout du support pour le schéma de document SSM version 2.2 dans EC2 ConfigUpdater• Ajout de la version du package AWS Nitro Enclaves au journal de la console• Nouvelle version de SSM Agent 3.0.529.0	4 mai 2021

Version	Détails	Date de publication
4.9.4326	<ul style="list-style-type: none">• Suppression de tous les liens dans l'interface utilisateur des paramètres• Il s'agit de la dernière version EC2Config qui prend en charge Windows Server 2008.	3 mars 2021
4.9.4279	<ul style="list-style-type: none">• Correction d'un problème de sécurité lié à la tâche <code>Ec2ConfigMonitor</code> planifiée• Correction du problème de mappage des lettres de lecteur et du nombre de disques éphémères incorrect• Ajout de <code>OsCurrentBuild</code> et <code>OsReleaseId</code> à la sortie de la console• Nouvelle version de SSM Agent 2.3.871.0	11 décembre 2020
4.9.4222	<ul style="list-style-type: none">• Correction de la logique de secours IMDS version 1.• Nouvelle version de SSM Agent 2.3.842.0	7 avril 2020
4.9.4122	<ul style="list-style-type: none">• Ajout de la prise en charge d'IMDS v2• Nouvelle version de SSM Agent 2.3.814.0	4 mars 2020
4.9.3865	<ul style="list-style-type: none">• Résolution du problème de détection du port COM pour Windows Server 2008 R2 sur les instances nues• Nouvelle version de SSM Agent 2.3.722.0	31 octobre 2019
4.9.3519	<ul style="list-style-type: none">• Nouvelle version de SSM Agent 2.3.634.0	18 juin 2019
4.9.3429	<ul style="list-style-type: none">• Nouvelle version de SSM Agent 2.3.542.0	25 avril 2019
4.9.3289	<ul style="list-style-type: none">• Nouvelle version de SSM Agent 2.3.444.0	11 février 2019

Version	Détails	Date de publication
4.9.3270	<ul style="list-style-type: none"> • Ajout d'un plugin afin que le moniteur ne s'éteigne jamais pour résoudre les problèmes ACPI • Édition et version du serveur SQL Server écrites dans la console • Nouvelle version de SSM Agent 2.3.415.0 	22 janvier 2019
4.9.3230	<ul style="list-style-type: none"> • Mise à jour de la description du mappage de lettres de lecteur pour mieux correspondre à la fonctionnalité. • Nouvelle version de SSM Agent 2.3.372.0 	10 janvier 2019
4.9.3160	<ul style="list-style-type: none"> • Temps d'attente accru pour la carte NIC principale • Ajout d'une configuration par défaut pour RSS et des paramètres de file d'attente de réception pour des périphériques ENA • Désactivation de la mise en veille prolongée lors de Sysprep • Nouvelle version de SSM Agent 2.3.344.0 • AWS SDK mis à jour vers la version 3.3.29.13 	15 décembre 2018
4.9.3067	<ul style="list-style-type: none"> • Améliorations apportées à la mise en veille prolongée d'instances • Nouvelle version de SSM Agent 2.3.235.0 	8 novembre 2018
4.9.3034	<ul style="list-style-type: none"> • Ajout de la route 169.254.169.253/32 pour le serveur DNS • Nouvelle version de SSM Agent 2.3.193.0 	24 octobre 2018
4.9.2986	<ul style="list-style-type: none"> • Ajout de la signature pour tous les fichiers binaires connexes EC2Config • Nouvelle version de SSM Agent 2.3.136.0 	11 octobre 2018
4.9.2953	Nouvelle version de SSM Agent (2.3.117.0)	2 octobre 2018
4.9.2926	Nouvelle version de SSM Agent (2.3.68.0)	18 septembre 2018

Version	Détails	Date de publication
4.9.2905	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.3.50.0) Ajout de la route 169.254.169.123/32 au service de temps AMZN Ajout de la route 169.254.169.249/32 au service de licence GRID Résolution d'un problème à cause duquel les volumes NVMe EBS étaient considérés comme éphémères 	17 septembre 2018
4.9.2854	Nouvelle version de SSM Agent (2.3.13.0)	17 août 2018
4.9.2831	Nouvelle version de SSM Agent (2.2.916.0)	7 août 2018
4.9.2818	Nouvelle version de SSM Agent (2.2.902.0)	31 juillet 2018
4.9.2756	Nouvelle version de SSM Agent (2.2.800.0)	27 juin 2018
4.9.2688	Nouvelle version de SSM Agent (2.2.607.0)	25 mai 2018
4.9.2660	Nouvelle version de SSM Agent (2.2.546.0)	11 mai 2018
4.9.2644	Nouvelle version de SSM Agent (2.2.493.0)	26 avril 2018
4.9.2586	Nouvelle version de SSM Agent (2.2.392.0)	28 mars 2018
4.9.2565	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.2.355.0) Problème sur les instances M5 et C5 (pilotes PV introuvables) Ajouter la journalisation de la console pour le type d'instance, les pilotes PV les plus récents et les pilotes NVMe 	13 mars 2018
4.9.2549	Nouvelle version de SSM Agent (2.2.325.0)	8 mars 2018
4.9.2461	Nouvelle version de SSM Agent (2.2.257.0)	15 février 2018
4.9.2439	Nouvelle version de SSM Agent (2.2.191.0)	6 février 2018

Version	Détails	Date de publication
4.9.2400	Nouvelle version de SSM Agent (2.2.160.0)	16 janvier 2018
4.9.2327	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.2.120.0) Ajout de la détection de port COM sur des instances matériel nu Amazon EC2 Ajout de la journalisation de statut Hyper-V sur des instances matériel nu Amazon EC2 	2 janvier 2018
4.9.2294	Nouvelle version de SSM Agent (2.2.103.0)	4 décembre 2017
4.9.2262	Nouvelle version de SSM Agent (2.2.93.0)	15 novembre 2017
4.9.2246	Nouvelle version de SSM Agent (2.2.82.0)	11 novembre 2017
4.9.2218	Nouvelle version de SSM Agent (2.2.64.0)	29 octobre 2017
4.9.2212	Nouvelle version de SSM Agent (2.2.58.0)	23 octobre 2017
4.9.2203	Nouvelle version de SSM Agent (2.2.45.0)	19 octobre 2017
4.9.2188	Nouvelle version de SSM Agent (2.2.30.0)	10 octobre 2017
4.9.2180	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.2.24.0) Ajout du plugin GPU Elastic pour les instances GPU 	5 octobre 2017
4.9.2143	Nouvelle version de SSM Agent (2.2.16.0)	1 octobre 2017
4.9.2140	Nouvelle version de SSM Agent (2.1.10.0)	
4.9.2130	Nouvelle version de SSM Agent (2.1.4.0)	

Version	Détails	Date de publication
4.9.2106	Nouvelle version de SSM Agent (2.0.952.0)	
4.9.2061	Nouvelle version de SSM Agent (2.0.922.0)	
4.9.2047	Nouvelle version de SSM Agent (2.0.913.0)	
4.9.2031	Nouvelle version de SSM Agent (2.0.902.0)	
4.9.2016	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.0.879.0) Correction du chemin du répertoire des CloudWatch journaux pour Windows Server 2003 	
4.9.1981	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.0.847.0) Correction du problème lié à la génération de fichier <code>important.txt</code> dans des volumes EBS. 	
4.9.1964	Nouvelle version de SSM Agent (2.0.842.0)	
4.9.1951	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.0.834.0) Correction du problème lié à l'absence de mappage de la lettre du lecteur à partir de Z: pour les disques éphémères. 	
4.9.1925	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.0.822.0) [Bogue] Cette version ne correspond pas à une cible de mise à jour valide de SSM Agent v4.9.1775. 	
4.9.1900	Nouvelle version de SSM Agent (2.0.805.0)	

Version	Détails	Date de publication
4.9.1876	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.0.796.0) Correction d'un problème lié à la redirection des sorties/erreurs pour l'exécution userdata administrateur. 	
4.9.1863	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.0.790.0) Correction de problèmes liés à la connexion de plusieurs volumes EBS à une instance Amazon EC2. CloudWatch Amélioré pour suivre un chemin de configuration, en conservant la rétrocompatibilité. 	
4.9.1791	Nouvelle version de SSM Agent (2.0.767.0)	
4.9.1775	Nouvelle version de SSM Agent (2.0.761.0)	
4.9.1752	Nouvelle version de SSM Agent (2.0.755.0)	
4.9.1711	Nouvelle version de SSM Agent (2.0.730.0)	
4.8.1676	Nouvelle version de SSM Agent (2.0.716.0)	
4.7.1631	Nouvelle version de SSM Agent (2.0.682.0)	
4.6.1579	<ul style="list-style-type: none"> Nouvelle version de SSM Agent (2.0.672.0) Le problème de mise à jour de l'agent a été résolu dans v4.3, v4.4 et v4.5 	
4.5.1534	Nouvelle version de SSM Agent (2.0.645.1)	
4.4.1503	Nouvelle version de SSM Agent (2.0.633.0)	
4.3.1472	Nouvelle version de SSM Agent (2.0.617.1)	

Version	Détails	Date de publication
4.2.1442	Nouvelle version de SSM Agent (2.0.599.0)	
4.1.1378	Nouvelle version de SSM Agent (2.0.558.0)	
4.0.1343	<ul style="list-style-type: none"> • Run Command, State Manager, l' CloudWatch agent et le support de jointure de domaine ont été transférés vers un autre agent appelé SSM Agent. SSM Agent sera installé dans le cadre de la mise à niveau d'EC2Config. Pour plus d'informations, consultez EC2Config et AWS Systems Manager. • Si vous avez un proxy configuré dans EC2Config, vous devrez mettre à jour vos paramètres de proxy pour SSM Agent avant la mise à niveau. Si vous ne mettez pas à jour les paramètres de proxy, vous ne pourrez pas utiliser la fonctionnalité Exécuter la commande pour gérer vos instances. Pour éviter ce problème, consultez les informations suivantes avant la mise à jour vers la nouvelle version : Installation et configuration de SSM Agent sur les instances Windows dans le Guide de l'utilisateur AWS Systems Manager . • Si vous avez précédemment activé CloudWatch l'intégration sur vos instances à l'aide d'un fichier de configuration local (<code>AWS.EC2.Windows.CloudWatch.json</code>), vous devrez configurer le fichier pour qu'il fonctionne avec l'agent SSM. 	
3.19.1153	<ul style="list-style-type: none"> • Plug-in d'activation réactivé pour les instances avec une ancienne AWS KMS configuration. Ignorez l'activation pour les utilisateurs BYOL. • Modifiez le comportement TRIM par défaut pour qu'il soit désactivé pendant le formatage du disque et ajoutez FormatWith TRIM pour remplacer le InitializeDisks plugin par userdata. 	

Version	Détails	Date de publication
3.18.1118	<ul style="list-style-type: none"> • Correctif permettant d'ajouter des routages à la carte réseau principale de manière fiable. • Mises à jour pour améliorer le support AWS des services. 	
3.17.1032	<ul style="list-style-type: none"> • Correctif qui résout le problème de duplication des journaux système lorsque les filtres étaient définis sur la même catégorie. • Correctifs empêchant toute suspension pendant l'initialisation du disque. 	
3.16.930	Prise en charge de la consignation de l'événement « Window is Ready to use » dans le journal d'événements Windows au démarrage.	
3.15.880	Correctif permettant de charger la sortie générée par la fonctionnalité Exécuter la commande de Systems Manager dans les compartiments S3 dont le nom inclut le caractère « . ».	
3.14.786	<p>Ajout du support pour remplacer les paramètres InitializeDisks du plugin. Par exemple : afin d'accélérer l'initialisation des disques SSD, vous pouvez désactiver temporairement TRIM en spécifiant cela dans userdata :</p> <pre>< InitializeDrives Paramètres>< SettingsGroup > FormatWithout SettingsGroup TRIM</ ></ Réglages InitializeDrives</pre>	
3.13.727	Fonctionnalité Exécuter la commande de Systems Manager : correctifs permettant de traiter les commandes en toute sécurité après le redémarrage de Windows.	

Version	Détails	Date de publication
3.12.649	<ul style="list-style-type: none">• Correctif permettant de traiter correctement le redémarrage lors de l'exécution de commandes/scripts.• Correctif permettant d'annuler en toute sécurité les commandes en cours d'exécution.• Prise en charge (le cas échéant) du chargement des journaux MSI dans S3 lors de l'installation des applications via la fonctionnalité Exécuter la commande de Systems Manager.	
3.11.521	<ul style="list-style-type: none">• Correctif permettant la génération d'empreintes numériques RDP pour Windows Server 2003.• Correctif permettant d'inclure un fuseau horaire et un décalage UTC dans les lignes de journal EC2Config.• Prise en charge de Systems Manager pour l'exécution des commandes Exécuter la commande en parallèle.• Restauration d'une modification précédente pour mettre en ligne les disques partitionnés.	
3.10.442	<ul style="list-style-type: none">• Correctif permettant de pallier les échec de configuration de Systems Manager lors de l'installation d'applications MSI.• Correctif permettant de mettre en ligne les disques de stockage en toute sécurité.• Mises à jour pour améliorer le support AWS des services.	

Version	Détails	Date de publication
3.9.359	<ul style="list-style-type: none">• Correctif du script Post-Sysprep afin de laisser la configuration de la mise à jour Windows dans un état par défaut.• Correctif apporté au plugin de génération de mot de passe pour améliorer la fiabilité de l'obtention des paramètres de politique de mot de passe GPO.• Limitation des autorisations de dossier de journal EC2Config/SSM au groupe d'administrateurs local.• Mises à jour pour améliorer le support AWS des services.	
3.8.294	<ul style="list-style-type: none">• Correction d'un problème CloudWatch qui empêchait le téléchargement des journaux lorsqu'ils ne se trouvaient pas sur le disque principal.• Amélioration du processus d'initialisation de disque en ajoutant une logique de nouvelle tentative.• Ajout d'une meilleure gestion des erreurs lorsque le SetPassword plugin échouait parfois lors de la création de l'AMI.• Mises à jour pour améliorer le support AWS des services.	

Version	Détails	Date de publication
3.7.308	<ul style="list-style-type: none">• Amélioration de l'utilitaire ec2config-cli pour les tests de configuration et le dépannage au sein de l'instance.• Évitez d'ajouter des routes statiques AWS KMS et un service de métadonnées sur un adaptateur OpenVPN.• Correction d'un problème où l'exécution des données utilisateur ne tenait pas compte de la balise « persist ».• Amélioration de la gestion des erreurs lorsque la connexion à la console EC2 n'est pas disponible.• Mises à jour pour améliorer le support AWS des services.	
3.6.269	<ul style="list-style-type: none">• Correctif de fiabilité de l'activation Windows afin d'utiliser l'adresse locale de lien 169.254.0.250/251 pour l'activation de Windows via AWS KMS• Amélioration de la gestion du proxy pour les scénarios Systems Manager, d'activation de Windows et de jonction de domaine• Correction d'un problème où les lignes dupliquées des comptes d'utilisateur étaient ajoutées au fichier de réponse Sysprep	
3.5.228	<ul style="list-style-type: none">• Résolution d'un scénario selon lequel le CloudWatch plugin consommait trop de CPU et de mémoire lors de la lecture des journaux d'événements Windows• Ajout d'un lien vers la documentation de CloudWatch configuration dans l'interface utilisateur des paramètres EC2Config	

Version	Détails	Date de publication
3.4.212	<ul style="list-style-type: none">• Correctifs apportés à EC2Config en cas d'utilisation combinée avec VM-Import.• Correction du problème de nom des services dans le programme d'installation WiX.	
3.3.174	<ul style="list-style-type: none">• Amélioration de la gestion des exceptions en cas d'échec au niveau de Systems Manager et de la jonction de domaine.• Modification pour prendre en charge la gestion des versions de schéma SSM de Systems Manager.• Correctif apporté au formatage des disques éphémères sur Win2K3.• Modification prenant en charge une taille de disque configuration supérieure à 2 To.• Réduction de l'utilisation de la mémoire virtuelle en affectant le mode GC par défaut.• Prise en charge du téléchargement des objets à partir du chemin d'accès UNC dans le plugin <code>aws:psModule</code> et <code>aws:application</code>.• Amélioration de la journalisation pour le plugin d'activation Windows.	

Version	Détails	Date de publication
3.2.97	<ul style="list-style-type: none">• Amélioration des performances en retardant le chargement des ensembles SSM de Systems Manager.• Amélioration de la gestion des exceptions pour les fichiers sysprep2008.xml mal formés.• Prise en charge de la ligne de commande pour la configuration de « Apply » dans Systems Manager.• Modification prenant en charge la jonction de domaine lorsque le changement de nom d'un ordinateur est en attente.• Prise en charge des paramètres facultatifs dans le plugin <code>aws:applications</code> .• Prise en charge du tableau de commande dans le plugin <code>aws:psModule</code> .	
3.0.54	<ul style="list-style-type: none">• Activer la prise en charge de Systems Manager.• Jonction de domaine automatique des instances EC2 Windows à un répertoire AWS via Systems Manager.• Configurez et téléchargez les CloudWatch logs/métriques via Systems Manager.• Installez PowerShell les modules via Systems Manager.• Installation des applications MSI via Systems Manager.	

Version	Détails	Date de publication
2.4.233	<ul style="list-style-type: none">• Ajout des tâches planifiées pour récupérer EC2Config en cas d'échec de démarrage du service.• Améliorations apportées aux messages d'erreur des journaux de la console.• Mises à jour pour améliorer le support AWS des services.	
2.3.313	<ul style="list-style-type: none">• Correction d'un problème lié à une consommation de mémoire importante dans certains cas lorsque la fonction CloudWatch Logs est activée.• Correction d'un bug de mise à niveau afin de permettre aux versions ec2config inférieures à 2.1.19 de passer à la dernière version.• Mise à jour de l'exception d'ouverture de port COM pour qu'elle soit plus descriptive et plus utile dans les journaux.• L'configServiceSettings interface utilisateur Ec2 a désactivé le redimensionnement et corrigé l'attribution et le placement de l'affichage des versions dans l'interface utilisateur.	
2.2.12	<ul style="list-style-type: none">• Gère NullPointerException lors de la requête d'une clé de registre pour déterminer l'état de Windows Sysprep qui renvoyait parfois null.• Libération des ressources non gérées dans un bloc final.	
2.2.11	Correction d'un problème lié à la gestion des lignes de journal vides dans le CloudWatch plugin.	

Version	Détails	Date de publication
2.2.10	<ul style="list-style-type: none"> • Suppression de la configuration CloudWatch des paramètres des journaux via l'interface utilisateur. • Permettez aux utilisateurs de définir CloudWatch les paramètres des journaux dans %ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json le fichier afin de permettre de futures améliorations. 	
2.2.9	Correctif de l'exception non gérée et ajout de la journalisation.	
2.2.8	<ul style="list-style-type: none"> • Correctifs apportés au contrôle de version du système d'exploitation Windows dans le programme d'installation EC2Config pour prendre en charge Windows Server 2003 SP1 ou version ultérieure. • Correctifs apportés à la gestion des valeurs null lors de la lecture des clés de registre liées à la mise à jour des fichiers de configuration Sysprep. 	
2.2.7	<ul style="list-style-type: none"> • Ajout de la prise en charge de l'exécution d'EC2Config au cours de l'exécution de Sysprep pour Windows 2008 ou version ultérieure. • Amélioration de la gestion des exceptions et de la journalisation pour des diagnostics plus précis 	
2.2.6	<ul style="list-style-type: none"> • Réduction de la charge sur l'instance et sur les CloudWatch journaux lors du téléchargement des événements du journal. • Résolution d'un problème de mise à niveau en raison duquel le plug-in CloudWatch Logs ne restait pas toujours activé 	

Version	Détails	Date de publication
2.2.5	<ul style="list-style-type: none">• Ajout de la prise en charge du téléchargement des journaux vers CloudWatch Log Service.• Correction d'un problème de condition de concurrence dans le plugin Ec2OutputRDPCert• Modification de l'option de restauration du service EC2Config pour redémarrer à partir de l'action TakeNo• Ajout d'informations d'exception en cas de plantage d'EC2Config	
2.2.4	<ul style="list-style-type: none">• Correction d'une faute de frappe dans PostSysprep le fichier .cmd• Correction du bug qui empêchait d'épingler EC2Config dans le menu Démarrer pour OS2012 ou version ultérieure	

Version	Détails	Date de publication
2.2.3	<ul style="list-style-type: none">• Ajout d'une option permettant d'installer EC2Config sans que le service ne démarre juste après l'installation. Pour l'utiliser, exécutez 'Ec2Install.exe start=false' à partir de l'invite de commande• Paramètre ajouté dans le plugin de fond d'écran pour contrôler l'ajout ou la suppression du fond d'écran. Pour l'utiliser, exécutez « Ec2 WallpaperInfo .exe set » ou « Ec2 WallpaperInfo .exe revert » à partir de l'invite de commande• Ajout de la vérification de RealTimelsUniversal la clé, affichage des paramètres incorrects de la clé de RealTimelsUniversal registre sur la console• Suppression de la dépendance EC2Config au dossier temporaire Windows• Suppression de la dépendance UserData d'exécution sur .Net 3.5	
2.2.2	<ul style="list-style-type: none">• Vérification supplémentaire du comportement d'arrêt du service afin de s'assurer que les ressources sont libérées• Correction d'un problème de lenteur d'exécution lors de la jonction à un domaine	

Version	Détails	Date de publication
2.2.1	<ul style="list-style-type: none">• Mise à jour du programme d'installation pour permettre les mises à niveau à partir des versions antérieures• Correction d'un WallpaperInfo bogue Ec2 dans l'environnement .Net4.5 uniquement• Correction du bug intermittent de détection des pilotes• Ajout de l'option d'installation en mode silencieux. Exécuter Ec2Install.exe avec l'option '-q' (par exemple, 'Ec2Install.exe -q')	
2.2.0	<ul style="list-style-type: none">• Ajout de la prise en charge des environnements .Net4 et .Net4.5• Mise à jour du programme d'installation	
2.1.19	<ul style="list-style-type: none">• Ajout de la prise en charge de l'étiquetage des disques éphémères en cas d'utilisation du pilote réseau Intel (par exemple, type d'instance C3). Pour plus d'informations, consultez Mise en réseau améliorée sur Amazon EC2.• Ajout de la prise en charge du nom et des versions des origines d'AMI dans la sortie de la console• Modifications apportées à la sortie de la console pour une analyse et une mise en forme cohérentes• Mise à jour du fichier d'aide	

Version	Détails	Date de publication
2.1.18	<ul style="list-style-type: none">• Ajout d'un objet WMI EC2Config pour la notification d'achèvement (-Namespace root \ Amazon -Class EC2_) ConfigService• Amélioration des performances de la requête de démarrage WMI avec les journaux d'événements volumineux ; susceptible d'entraîner une utilisation de l'UC élevée et prolongée au cours de l'exécution initiale	
2.1.17	<ul style="list-style-type: none">• Correction UserData d'un problème d'exécution avec le remplissage de la mémoire tampon en sortie standard et en erreur standard• Correction de l'empreinte numérique RDP incorrect qui figure parfois la sortie e la console pour le système d'exploitation >= w2k8• La sortie console contient désormais « RDPCERTIFICATE-SubjectName : » pour Windows 2008+, qui contient la valeur du nom de la machine• Ajout de D:\ dans le menu déroulant de mappage de lettres de lecteur• Déplacement du bouton d'aide en haut à droite et modification de l'aspect de l'interface• Ajout d'un lien renvoyant vers une enquête utilisateur en haut à droite	

Version	Détails	Date de publication
2.1.16	<ul style="list-style-type: none">• L'onglet General comprend un lien vers la page de téléchargement d'EC2Config pour les nouvelles versions• La superposition de papier peint du bureau est désormais stockée dans le dossier Appdata local des utilisateurs au lieu de Mes documents pour permettre la redirection MyDoc• Synchronisation du nom MSSQLServer avec système dans le script Post-Sysprep (2008 ou version ultérieure)• Réorganisation du dossier d'application (transfert des fichiers vers le répertoire Plugin et suppression des fichiers dupliqués)• Modification de la sortie du journal système (console) :• *Activation d'un format de date, de nom ou de valeur pour faciliter l'analyse (veuillez commencer la migration des dépendances vers le nouveau format)• * Ajout du statut du plugin « Ec2 SetPassword »• * Ajouté des heures de début et de fin Sysprep• Correction d'un problème empêchant l'étiquetage des disques éphémères en tant que « stockage temporaire » pour les systèmes d'exploitation non anglophones• Correction de l'échec de désinstallation d'EC2Config après l'exécution de Sysprep	

Version	Détails	Date de publication
2.1.15	<ul style="list-style-type: none">• Requêtes optimisées pour le service de métadonnées• Les métadonnées contournent maintenant les paramètres de proxy• Placement des disques éphémères étiquetés en tant que « stockage temporaire » et Important.txt sur volume le lorsqu'ils sont détectés (pilotes PV Citrix uniquement). Pour plus d'informations, consultez Mise à niveau des pilotes PV sur les instances Windows.• Attribution des lettres de lecteurs Z à A aux disques éphémères (pilotes PV Citrix uniquement) : cette attribution peut être remplacée à l'aide du plugin de mappage de lettres de lecteur avec les volumes dont l'étiquette indique « Stockage temporaire X », où x est un nombre compris entre 0 et 25• UserData s'exécute désormais immédiatement après « Windows est prêt »	
2.1.14	Correctifs apportés au fond d'écran du Bureau	
2.1.13	<ul style="list-style-type: none">• Le fond d'écran du Bureau affiche le nom d'hôte par défaut• Suppression de la dépendance au service d'horloge Windows• Ajoute du routage lorsque plusieurs adresses IP sont attribuées à une seule interface	

Version	Détails	Date de publication
2.1.11	<ul style="list-style-type: none"> • Modifications apportées au plugin Ec2Activation • - Vérifie l'état d'activation tous les 30 jours • - S'il reste 90 jours (sur 180) pour la période de grâce, tente une nouvelle activation 	
2.1.10	<ul style="list-style-type: none"> • La superposition du fond d'écran sur le Bureau ne persiste plus avec Sysprep ou en cas de fermeture sans Sysprep • Exécution de l'option UserData à chaque démarrage du service avec <code><persist>true</persist></code> • Emplacement et nom modifiés de/DisableWinUpdate.cmd en /Scripts/ .cmd PostSysprep • Le mot de passe administrateur est configuré pour ne pas expirer par défaut dans PostSysprep /Scripts/ .cmd • La désinstallation supprimera le PostSysprep script EC2Config de c:\windows\setup\script \ .cmd CommandComplete • L'ajout du routage prend en charge les métriques d'interface personnalisées 	
2.1.9	UserData L'exécution n'est plus limitée à 3851 caractères	

Version	Détails	Date de publication
2.1.7	<ul style="list-style-type: none">• Écriture de l'identifiant de langue et de version du système d'exploitation dans la console• Écriture de la version d'EC2Config dans la console• Écriture de la version du pilote PV dans la console• Détection de la vérification des bugs et, le cas échéant, envoi à la console lors du démarrage suivant• Ajout d'une option à config.xml afin de rendre persistantes les informations d'identification Sysprep• Ajout d'une logique de nouvelle tentative de routage en cas d'indisponibilité des ENI au démarrage• Écriture du PID d'exécution des données utilisateur dans la console• Récupération de la longueur minimale des mots de passe générés à partir de la stratégie de groupe• Définition de 3 tentatives de démarrage du service• Ajout d'exemples de fichiers S3_ DownloadFile .ps1 et S3_Upload .ps1 dans le dossier /Scripts	

Version	Détails	Date de publication
2.1.6	<ul style="list-style-type: none">• Ajout des informations de version dans l'onglet General• Remplacement du nom de l'onglet Bundle par Image• Simplification du processus de spécification des mots de passe et transfert de l'interface utilisateur liée aux mots de passe dans l'onglet Image au lieu de l'onglet General• Remplacement du nom de l'onglet Disk Settings par Storage• Ajout d'un onglet Support offrant des outils communs permettant de résoudre les problèmes• Configuration de Windows Server 2003 <code>sysprep.ini</code> pour étendre par défaut la partition du système d'exploitation• Ajout de l'adresse IP privée au fond d'écran• Affichage de l'adresse IP privée sur le fond d'écran• Ajout d'une logique de nouvelle tentative pour la sortie de la console• Correction de l'exception de port COM pour l'accessibilité des métadonnées, qui entraînait l'arrêt d'EC2Config avant l'affichage de la sortie de la console• Vérification de l'état d'activation à chaque démarrage (activation si nécessaire)• Correction du problème lié aux chemins d'accès relatifs, qui survenait lors de l'exécution manuelle d'un raccourci de fond d'écran à partir du dossier de démarrage, renvoyant vers <code>Administrator/logs</code>	

Version	Détails	Date de publication
	<ul style="list-style-type: none">• Correction de la couleur d'arrière-plan par défaut pour les utilisateurs Windows Server 2003 (autre qu'administrateurs)	

Version	Détails	Date de publication
2.1.2	<ul style="list-style-type: none">• Horodatages de la console en UTC (Zulu)• Suppression de l'affichage du lien hypertexte dans l'onglet Sysprep• Ajout d'une fonctionnalité afin d'étendre dynamiquement le volume racine lors du premier démarrage de Windows 2008 ou version ultérieure• Lorsque Set-Password est activé, EC2Config peut maintenant définir automatiquement le mot de passe• EC2Config vérifie l'état d'activation avant d'exécuter Sysprep (génère un avertissement si cette fonctionnalité n'est pas activée)• Sysprep.xml Windows Server 2003 utilise maintenant le fuseau horaire UTC par défaut au lieu de celui du Pacifique• Serveurs d'activation aléatoires• Remplacement du nom de l'onglet Drive Mapping par Disk Settings• Transfert des éléments d'interface d'initialisation des disques dans l'onglet Disk Settings à partir de l'onglet General• Le bouton d'aide renvoie maintenant vers le fichier d'aide HTML• Mise à jour du fichier d'aide HTML• Mise à jour du texte « Note » pour les mappages de lettres de lecteur	

Version	Détails	Date de publication
	<ul style="list-style-type: none">• Ajout du InstallUpdates fichier .ps1 au dossier /Scripts pour automatiser les correctifs et le nettoyage avant Sysprep	
2.1.0	<ul style="list-style-type: none">• Le fond d'écran du Bureau affiche les informations d'instance par défaut dès la première connexion (pas en cas de déconnexion et de reconnexion)• PowerShell peut être exécuté à partir des données utilisateur en entourant le code avec <code><powershell></powershell></code>	

S'abonner aux notifications du service EC2Config

Amazon SNS peut vous notifier en cas de publication de nouvelles versions du service EC2Config. Pour vous abonner à ces notifications, utilisez la procédure suivante.

Pour s'abonner aux notifications d'EC2Config

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région, car les notifications SNS auxquelles vous vous abonnez ont été créées dans cette région.
3. Dans le panneau de navigation, choisissez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :
 - a. Pour ARN de la rubrique, utilisez l'Amazon Resource Name (ARN) suivant :

```
arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
```

- b. Pour Protocole, choisissez Email.
- c. Pour Point de terminaison, tapez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications.

- d. Choisissez Créer un abonnement.
6. Vous recevrez un e-mail vous demandant de confirmer votre abonnement. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Chaque fois qu'une nouvelle version du service EC2Config est publiée, nous envoyons des notifications aux abonnés de la rubrique. Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Pour annuler votre abonnement aux notifications d'EC2Config

1. Ouvrez la console Amazon SNS.
2. Dans le panneau de navigation, choisissez Abonnements.
3. Sélectionnez l'abonnement, puis choisissez Actions, Delete subscriptions (Supprimer les abonnements). Lorsque vous êtes invité à confirmer, choisissez Delete (Supprimer).

Résoudre les problèmes liés au service EC2Config

Les informations suivantes peuvent vous aider à résoudre les problèmes liés au service EC2Config.

Mettre à jour EC2Config sur une instance inaccessible

Utilisez la procédure suivante pour mettre à jour le service EC2Config sur une instance Windows Server inaccessible à l'aide des services Bureau à distance.

Pour mettre à jour EC2Config sur une instance Windows basée sur des volumes Amazon EBS à laquelle vous ne parvenez pas à vous connecter

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Recherchez l'instance concernée. Sélectionnez l'instance, État de l'instance, puis Arrêter l'instance.

 Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

- Sélectionnez Lancer des instances et créez une instance `t2.micro` temporaire dans la même zone de disponibilité que l'instance affectée. Utilisez une autre AMI que celle que vous avez utilisée pour lancer l'instance concernée.

 Important

Si vous ne créez pas l'instance dans la même zone de disponibilité que l'instance affectée, vous ne pourrez pas attacher le volume racine de celle-ci à la nouvelle instance.

- Dans la console EC2, choisissez Volumes.
- Recherchez le volume racine de l'instance affectée. Détachez le volume et attachez-le à l'instance temporaire que vous avez créée précédemment. Attachez-le avec le nom du périphérique par défaut (`xvdf`).
- Utilisez les services Bureau à distance pour vous connecter à l'instance temporaire, puis utilisez l'utilitaire Gestion des disques pour rendre le volume disponible.
- [Téléchargez](#) la version la plus récente du service EC2Config. Extrayez les fichiers du fichier `.zip` dans le répertoire Temp du lecteur que vous avez attaché.
- Sur l'instance temporaire, ouvrez la boîte de dialogue Run (Exécuter), tapez **regedit** et appuyez sur Entrée.
- Sélectionnez `HKEY_LOCAL_MACHINE`. Dans le menu File (Fichier), choisissez Load Hive (Charger Hive). Choisissez le lecteur, puis accédez au fichier `Windows\System32\config\SOFTWARE` et ouvrez-le. Quand vous y êtes invité, spécifiez un nom de clé.
- Sélectionnez la clé que vous venez de charger et naviguez jusqu'à `Microsoft\Windows\CurrentVersion`. Choisissez la clé `RunOnce`. Si elle n'existe pas, choisissez `CurrentVersion` dans le menu contextuel (clic droit), choisissez Nouveau, puis Clé. Nommez la clé `RunOnce`.
- Dans le menu contextuel (clic droit), choisissez la clé `RunOnce`, Nouveau, puis Valeur de chaîne. Entrez le nom `Ec2Install` et les données `C:\Temp\Ec2Install.exe /quiet`.
- Choisissez la clé `HKEY_LOCAL_MACHINE\specified key name\Microsoft\Windows NT\CurrentVersion\Winlogon`. Dans le menu contextuel (clic droit), choisissez Nouveau, puis Valeur de chaîne. Entrez le nom **AutoAdminLogon** et les données **1**.
- Choisissez la clé `HKEY_LOCAL_MACHINE\specified key name\Microsoft\Windows NT\CurrentVersion\Winlogon>`. Dans le menu contextuel (clic droit), choisissez Nouveau, puis Valeur de chaîne. Entrez le nom **DefaultUserName** et les données **Administrator**.

15. Choisissez la clé HKEY_LOCAL_MACHINE*specified key name*\Microsoft\Windows NT \CurrentVersion\Winlogon. Dans le menu contextuel (clic droit), choisissez Nouveau, puis Valeur de chaîne. Entrez le nom **DefaultPassword** ainsi qu'un mot de passe dans les données de la valeur.
16. Dans le volet de navigation de l'Éditeur du Registre, choisissez la clé temporaire que vous avez créée lorsque vous avez ouvert pour la première fois l'Éditeur du Registre.
17. Dans le menu File (Fichier), choisissez Unload Hive (Décharger Hive).
18. Dans l'utilitaire Gestion des disques, choisissez le lecteur que vous avez attaché précédemment, ouvrez le menu contextuel (clic droit) et choisissez Hors connexion.
19. Dans la console Amazon EC2, détachez le volume affecté de l'instance temporaire et rattachez-le à votre instance sous le nom de périphérique /dev/sda1. Vous devez spécifier ce nom de périphérique pour désigner le volume en tant que volume racine.
20. [Arrêtez et démarrez les instances Amazon EC2](#) l'instance.
21. Une fois l'instance démarrée, consultez le journal système et vérifiez que le message Windows is ready to use est affiché.
22. Ouvrez l'Éditeur du Registre et choisissez HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows NT\CurrentVersion\Winlogon. Supprimez les clés String Value que vous avez créées précédemment : AutoAdminLogon, DefaultUserName et DefaultPassword.
23. Supprimez ou arrêtez l'instance temporaire que vous avez créée au cours de cette procédure.

Utilisez EC2 Fast Launch pour vos instances Windows

Chaque instance Windows Amazon EC2 doit passer par les étapes de lancement standard du système d'exploitation Windows, qui comprennent plusieurs redémarrages et prennent souvent 15 minutes ou plus. Les AMI Windows Server Amazon EC2 sur lesquelles la fonctionnalité EC2 Fast Launch est activée effectuent certaines de ces étapes et redémarrent à l'avance afin de réduire le temps nécessaire au lancement d'une instance.

Lorsque vous configurez une AMI Windows Server pour EC2 Fast Launch, Amazon EC2 crée un ensemble de snapshots préconfigurés à utiliser pour un lancement plus rapide, comme suit.

1. Amazon EC2 lance un ensemble d'instances t3 temporaires, en fonction de vos paramètres.
2. Lorsque chaque instance temporaire effectue les étapes de lancement standard, Amazon EC2 crée un instantané pré-approvisionné de l'instance. Il stocke l'instantané dans votre compartiment Amazon S3.

3. Lorsque l'instantané est prêt, Amazon EC2 met fin à l'instance t3 associée afin de maintenir les coûts de ressources aussi bas que possible.
4. La prochaine fois qu'Amazon EC2 lancera une instance à partir de l'AMI compatible EC2 Fast Launch, il utilisera l'un des instantanés pour réduire considérablement le temps de lancement.

Amazon EC2 réapprovisionne automatiquement les instantanés que vous avez sous la main lorsqu'il les utilise pour lancer des instances à partir de l'AMI compatible avec EC2 Fast Launch.

Tout compte ayant accès à une AMI avec EC2 Fast Launch activé peut bénéficier de délais de lancement réduits. Lorsque le propriétaire de l'AMI vous autorise à lancer des instances, les instantanés pré-alloués proviennent du compte du propriétaire de l'AMI.

Si une AMI compatible avec EC2 Fast Launch est partagée avec vous, vous pouvez activer ou désactiver vous-même le lancement plus rapide sur l'AMI partagée. Si vous activez une AMI partagée pour EC2 Fast Launch, Amazon EC2 crée les instantanés préconfigurés directement dans votre compte. Si vous supprimez les instantanés de votre compte, vous pouvez toujours utiliser les instantanés du compte du propriétaire de l'AMI.

Note

EC2 Fast Launch supprime les instantanés préprovisionnés dès qu'ils sont consommés par un lancement afin de minimiser les coûts de stockage et d'empêcher leur réutilisation. Toutefois, si les instantanés supprimés répondent à une règle de conservation, la Corbeille les conserve automatiquement. Nous vous recommandons de revoir le champ d'application de vos règles de conservation de la corbeille afin d'éviter que cela ne se produise. Pour plus d'informations, consultez [Considérations](#).

Cette fonctionnalité n'est pas la même que la [restauration rapide d'instantanés EBS](#). La restauration rapide d'instantanés EBS doit être explicitement activée pour chaque instantané, et a ses propres coûts associés.

La vidéo suivante explique comment configurer votre AMI Windows pour un lancement plus rapide avec un bref aperçu des termes clés associés et de leurs définitions : [Lancer des instances Windows EC2 jusqu'à 65 % plus rapidement](#). AWS

Coûts des ressources

La configuration des AMI Windows pour EC2 Fast Launch est gratuite. Toutefois, la tarification standard s'applique à toutes les AWS ressources sous-jacentes utilisées par Amazon EC2. Pour en savoir plus sur les coûts de ressources associés et sur la façon de les gérer, consultez [Gérez les coûts des ressources avec EC2 Fast Launch](#).

Table des matières

- [Termes clés](#)
- [Conditions préalables au lancement rapide d'EC2](#)
- [Configurer les paramètres de lancement rapide EC2 pour votre AMI Amazon EC2 Windows Server](#)
- [Afficher les AMI avec EC2 Fast Launch activé](#)
- [Gérez les coûts des ressources avec EC2 Fast Launch](#)
- [Lancement rapide du moniteur EC2](#)
- [Rôle lié au service pour EC2 Fast Launch](#)

Termes clés

La fonction EC2 Fast Launch utilise les termes clés suivants :

Instantané pré-approvisionné

Un instantané d'une instance qui a été lancée à partir d'une AMI Windows avec EC2 Fast Launch activé, et qui a effectué les étapes de lancement Windows suivantes, en redémarrant selon les besoins.

- Sysprep specialize
- OOBE (Windows Out of Box Experience)

Lorsque ces étapes sont terminées, EC2 Fast Launch arrête l'instance et crée un instantané qui est ensuite utilisé pour un lancement plus rapide depuis l'AMI, en fonction de votre configuration.

Fréquence de lancement

Contrôle le nombre d'instantanés pré-approvisionnés qu'Amazon EC2 peut lancer dans le laps de temps spécifié. Lorsque vous activez EC2 Fast Launch pour votre AMI, Amazon EC2 crée l'ensemble initial de snapshots préprovisionnés en arrière-plan. Par exemple, si la fréquence de lancement est définie sur cinq lancements par heure, ce qui est la valeur par défaut, EC2 Fast Launch crée un ensemble initial de cinq instantanés préprovisionnés.

Lorsqu'Amazon EC2 lance une instance depuis une AMI avec EC2 Fast Launch activé, il utilise l'un des snapshots préprovisionnés pour réduire le temps de lancement. Au fur et à mesure que les instantanés sont utilisés, ils sont automatiquement réapprovisionnés, jusqu'au nombre spécifié par la fréquence de lancement.

Si vous vous attendez à un pic du nombre d'instances lancées depuis votre AMI (lors d'un événement spécial, par exemple), vous pouvez augmenter la fréquence de lancement à l'avance pour couvrir les instances supplémentaires dont vous aurez besoin. Lorsque votre cadence de lancement revient à la normale, vous pouvez réajuster la fréquence à la baisse.

Lorsque le nombre de lancements est plus élevé que prévu, vous risquez d'épuiser tous les instantanés pré-approvisionnés dont vous disposez. Cela ne provoque pas d'échec des lancements. Cependant, il peut arriver que certaines instances passent par le processus de lancement standard, jusqu'à ce que les instantanés puissent être réapprovisionnés.

Nombre de ressources cible

Le nombre de snapshots préprovisionnés à conserver à portée de main pour une AMI Amazon EC2 Windows Server avec EC2 Fast Launch activé.

Nombre maximal de lancements parallèles

Contrôle le nombre d'instances qu'Amazon EC2 peut lancer en même temps afin de créer les instantanés préprovisionnés pour EC2 Fast Launch. Si votre nombre de ressources cible est supérieur au nombre maximum de lancements parallèles que vous avez configuré, Amazon EC2 lance initialement le nombre d'instances spécifié par le nombre de lancements parallèles maximum pour commencer à créer les instantanés. Lorsque ces instances terminent le processus, Amazon EC2 prend l'instantané et arrête l'instance. Il continue ensuite à lancer d'autres instances jusqu'à ce que le nombre total d'instantanés disponibles atteigne le nombre de ressources cible. La valeur pour Nombre maximal de lancements parallèles doit être supérieur ou égal à 6.

Conditions préalables au lancement rapide d'EC2

Avant de configurer EC2 Fast Launch, vérifiez que vous remplissez les conditions préalables suivantes qui sont requises pour créer des instantanés pour les AMI de votre : Compte AWS

- Si vous n'utilisez pas de modèle de lancement pour configurer vos paramètres, assurez-vous qu'un VPC par défaut est configuré pour la région dans laquelle vous utilisez EC2 Fast Launch.

Note

Si vous supprimez accidentellement votre VPC par défaut dans la région dans laquelle vous prévoyez de configurer EC2 Fast Launch, vous pouvez créer un nouveau VPC par défaut dans cette région. Pour en savoir plus, consultez [Créer un VPC par défaut](#) dans le Guide de l'utilisateur Amazon VPC.

- Pour spécifier un autre VPC que celui par défaut, vous devez utiliser un modèle de lancement lorsque vous configurez le lancement rapide de Windows. Pour plus d'informations, consultez [Utiliser un modèle de lancement lorsque vous configurez EC2 Fast Launch](#).
- Si votre compte inclut une politique qui applique IMDSv2 pour les instances Amazon EC2, vous devez créer un modèle de lancement qui spécifie la configuration des métadonnées pour appliquer IMDSv2.
- Les AMI privées EC2 Fast Launch doivent prendre en charge l'exécution de scripts de données utilisateur.
- Pour configurer EC2 Fast Launch pour une AMI, vous devez créer l'AMI à l'option d'arrêt de l'option d'arrêt. La fonctionnalité EC2 Fast Launch ne prend actuellement pas en charge les AMI créées à partir d'une instance en cours d'exécution.

Pour créer une AMI à l'aide de Sysprep, consultez [Création d'une AMI avec Windows Sysprep](#).

- Le quota par défaut pour le Nombre maximal de lancements parallèles sur toutes les AMI d'un Compte AWS est de 40 par région. Vous pouvez demander une augmentation des Service Quotas pour votre compte, comme suit.
 1. Connectez-vous à la console Service Quotas AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/servicequotas/>.
 2. Dans le panneau de navigation, sélectionnez Services AWS.
 3. Dans la barre de recherche, saisissez EC2 Fast Launch, puis sélectionnez le résultat.
 4. Sélectionnez le lien pour Parallel instance launches. Cela vous dirige vers la page détaillée Service Quotas du Lancement d'instances parallèles.
 5. Choisissez Request quota increase (Demander une augmentation de quota).

Pour de plus amples informations, veuillez consulter [Demande d'augmentation de quota](#) dans le Guide de l'utilisateur Service Quotas.

Configurer les paramètres de lancement rapide EC2 pour votre AMI Amazon EC2 Windows Server

Vous pouvez configurer EC2 Fast Launch pour les AMI Windows dont vous êtes propriétaire ou les AMI partagées avec vous à partir de l'API AWS Management Console CloudFormation, des SDK ou AWS Command Line Interface (AWS CLI). Avant de configurer EC2 Fast Launch, vérifiez que votre AMI répond à toutes les conditions requises pour créer les instantanés préprovisionnés. Pour plus d'informations, consultez [Conditions préalables au lancement rapide d'EC2](#).

Les sections suivantes décrivent les étapes de configuration de la console Amazon EC2 et AWS CLI

Activer le lancement rapide d'EC2

Pour activer EC2 Fast Launch, choisissez l'onglet correspondant à votre environnement, puis suivez les étapes.

Note

Avant de modifier ces paramètres, assurez-vous que votre AMI et la région dans laquelle vous l'exécutez sont conformes à tous les [Conditions préalables au lancement rapide d'EC2](#).

Console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Images, choisissez AMIs (AMI).
3. Sélectionnez l'AMI à mettre à jour en cochant la case en regard de Name (Nom).
4. Dans le menu Actions situé au-dessus de la liste des AMI, choisissez Configurer le lancement rapide. Cela ouvre la page Configurer le lancement rapide, dans laquelle vous configurez les paramètres du lancement rapide EC2.
5. Pour commencer à utiliser des instantanés pré-approvisionnés afin de lancer des instances à partir de votre AMI Windows plus rapidement, cochez la case Activer le lancement rapide de Windows.
6. Depuis la liste déroulante Set anticipated launch frequency (Définir une fréquence de lancement prévue), choisissez une valeur afin de spécifier le nombre d'instantanés créés et gérés pour couvrir le volume de lancement d'instances attendu.
7. Une fois les modifications terminées, choisissez Save changes (Enregistrer les modifications).

Note

Si vous devez utiliser un modèle de lancement pour spécifier un autre VPC que celui par défaut ou pour configurer les paramètres de métadonnées pour IMDSv2, consultez [Utiliser un modèle de lancement lorsque vous configurez EC2 Fast Launch](#).

AWS CLI

La `enable-fast-launch` commande appelle l'opération d'API Amazon EC2 [EnableFastLaunch](#).

Syntaxe :

```
aws ec2 enable-fast-launch \  
  --image-id <value> \  
  --resource-type <value> \ (optional)  
  --snapshot-configuration <value> \ (optional)  
  --launch-template <value> \ (optional)  
  --max-parallel-launches <value> \ (optional)  
  --dry-run | --no-dry-run \ (optional)  
  --cli-input-json <value> \ (optional)  
  --generate-cli-skeleton <value> \ (optional)
```

Exemple :

L'exemple d'[activation rapide suivant active le lancement rapide](#) d'EC2 pour l'AMI spécifiée, en lançant six instances parallèles pour le pré-provisionnement. `ResourceType` est défini sur `snapshot`, qui est la valeur par défaut.

```
aws ec2 enable-fast-launch \  
  --image-id ami-01234567890abcdef \  
  --max-parallel-launches 6 \  
  --resource-type snapshot
```

Sortie :

```
{  
  "ImageId": "ami-01234567890abcdef",  
  "ResourceType": "snapshot",  
  "SnapshotConfiguration": {
```

```

    "TargetResourceCount": 10
  },
  "LaunchTemplate": {},
  "MaxParallelLaunches": 6,
  "OwnerId": "0123456789123",
  "State": "enabling",
  "StateTransitionReason": "Client.UserInitiated",
  "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
}

```

Tools for PowerShell

L'`Enable-EC2FastLaunch` de commande appelle l'opération d'API Amazon [EnableFastEC2Launch](#) pour activer le lancement rapide d'EC2 sur votre AMI Windows.

Syntaxe :

```

Enable-EC2FastLaunch
  -ImageId <String>
  -LaunchTemplate_LaunchTemplateId <String>
  -LaunchTemplate_LaunchTemplateName <String>
  -MaxParallelLaunch <Int32>
  -ResourceType <String>
  -SnapshotConfiguration_TargetResourceCount <Int32>
  -LaunchTemplate_Version <String>
  -Select <String>
  -PassThru <SwitchParameter>
  -Force <SwitchParameter>

```

Exemple :

L'[Enable-EC2FastLaunch](#) exemple suivant active le lancement rapide d'EC2 pour l'AMI spécifiée, en lançant six instances parallèles pour le pré-provisionnement. `ResourceType` est défini sur `snapshot`, qui est la valeur par défaut.

```

Enable-EC2FastLaunch `
  -ImageId ami-01234567890abcdef `
  -MaxParallelLaunch 6 `
  -Region us-west-2 `
  -ResourceType snapshot

```

Sortie :

```
ImageId           : ami-01234567890abcdef
LaunchTemplate    :
MaxParallelLaunches : 6
OwnerId          : 0123456789123
ResourceType     : snapshot
SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
State            : enabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime  : 2/25/2022 12:24:11 PM
```

Désactiver le lancement rapide d'EC2

Pour désactiver EC2 Fast Launch, choisissez l'onglet correspondant à votre environnement, puis suivez les étapes.

Note

Avant de modifier ces paramètres, assurez-vous que votre AMI et la région dans laquelle vous l'exécutez sont conformes à tous les [Conditions préalables au lancement rapide d'EC2](#).

Console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Images, choisissez AMIs (AMI).
3. Sélectionnez l'AMI à mettre à jour en cochant la case en regard de Name (Nom).
4. Dans le menu Actions situé au-dessus de la liste des AMI, choisissez Configurer le lancement rapide. Cela ouvre la page Configurer le lancement rapide, dans laquelle vous configurez les paramètres du lancement rapide EC2.
5. Décochez la case Activer le lancement rapide pour Windows pour désactiver le lancement rapide d'EC2 et pour supprimer les instantanés préprovisionnés. L'AMI utilise désormais le processus de lancement standard pour chaque instance.

Note

Lorsque vous désactivez l'optimisation des images Windows, tous les instantanés pré-approvisionnés existants sont automatiquement supprimés. Vous devez terminer cette étape pour recommencer à utiliser la fonction.

- Une fois les modifications terminées, choisissez Save changes (Enregistrer les modifications).

AWS CLI

La `disable-fast-launch` commande appelle l'opération d'API Amazon EC2 [DisableFastLaunch](#).

Syntaxe :

```
aws ec2 disable-fast-launch \  
  --image-id <value> \  
  --force | --no-force \ (optional)  
  --dry-run | --no-dry-run \ (optional)  
  --cli-input-json <value> \ (optional)  
  --generate-cli-skeleton <value> \ (optional)
```

Exemple :

L'exemple de [désactivation rapide suivant désactive le lancement rapide](#) d'EC2 sur l'AMI spécifiée et nettoie les snapshots préprovisionnés existants.

```
aws ec2 disable-fast-launch \  
  --image-id ami-01234567890abcdef
```

Sortie :

```
{  
  "ImageId": "ami-01234567890abcdef",  
  "ResourceType": "snapshot",  
  "SnapshotConfiguration": {},  
  "LaunchTemplate": {  
    "LaunchTemplateId": "lt-01234567890abcdef",  
    "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-  
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
```

```
    "Version": "1"
  },
  "MaxParallelLaunches": 6,
  "OwnerId": "0123456789123",
  "State": "disabling",
  "StateTransitionReason": "Client.UserInitiated",
  "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
}
```

Tools for PowerShell

L'[Disable-EC2FastLaunch](#) applet de commande appelle l'opération d'API Amazon [DisableFastEC2Launch](#).

Syntaxe :

```
Disable-EC2FastLaunch
  -ImageId <String>
  -ForceStop <Boolean>
  -Select <String>
  -PassThru <SwitchParameter>
  -Force <SwitchParameter>
```

Exemple :

L'[Disable-EC2FastLaunch](#) exemple suivant désactive EC2 Fast Launch sur l'AMI spécifiée et nettoie les snapshots préprovisionnés existants.

```
Disable-EC2FastLaunch -ImageId ami-01234567890abcdef
```

Sortie :

```
ImageId           : ami-01234567890abcdef
LaunchTemplate    :
Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches : 6
OwnerId           : 0123456789123
ResourceType      : snapshot
SnapshotConfiguration :
State             : disabling
```

```
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Utiliser un modèle de lancement lorsque vous configurez EC2 Fast Launch

Avec un modèle de lancement, vous pouvez configurer un ensemble de paramètres de lancement qu'Amazon EC2 utilise chaque fois qu'il lance une instance à partir de ce modèle. Vous pouvez spécifier des éléments tels qu'une AMI à utiliser pour l'image de base, les types d'instance, le stockage, les paramètres réseau, etc.

Les modèles de lancement sont facultatifs, sauf dans les cas spécifiques suivants, où vous devez utiliser un modèle de lancement pour votre AMI Windows lorsque vous configurez un lancement plus rapide :

- Vous devez utiliser un modèle de lancement afin de spécifier un autre VPC que celui par défaut pour votre AMI Windows.
- Si votre compte inclut une politique qui applique IMDSv2 pour les instances Amazon EC2, vous devez créer un modèle de lancement qui spécifie la configuration des métadonnées pour appliquer IMDSv2.

[Utilisez le modèle de lancement qui inclut votre configuration de métadonnées depuis la console EC2, ou lorsque vous exécutez la commande `enable-fast-launch` dans le AWS CLI, ou lorsque vous appelez l'EnableFastaction Launch API.](#)

Amazon EC2 Fast Launch ne prend pas en charge la configuration suivante lorsque vous utilisez un modèle de lancement. Si vous utilisez un modèle de lancement pour EC2 Fast Launch, vous ne devez spécifier aucun des éléments suivants :

- Scripts de données utilisateur
- Protection de la résiliation
- Métadonnées désactivées
- Option spot
- Comportement d'arrêt qui met fin à l'instance
- Balises de ressources pour les demandes d'interface réseau, d'Elastic Graphic ou d'instance ponctuelle

Spécifier un autre VPC que celui par défaut

Étape 1 : créer un modèle de lancement

Créez un modèle de lancement qui spécifie les informations suivantes pour vos instances Windows :

- Le sous-réseau VPC.
- Un type d'instance de `t3.xlarge`.

Pour plus d'informations, consultez [Création d'un modèle de lancement](#).

Étape 2 : Spécifiez le modèle de lancement pour votre AMI EC2 Fast Launch

Choisissez l'onglet qui correspond à votre processus :

Console

Pour spécifier le modèle de lancement d'EC2 Fast Launch à partir du AWS Management Console, procédez comme suit :

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Images, choisissez AMIs (AMI).
3. Sélectionnez l'AMI à mettre à jour en cochant la case en regard de Name (Nom).
4. Dans le menu Actions situé au-dessus de la liste des AMI, choisissez Configurer le lancement rapide. Cela ouvre la page Configurer le lancement rapide, dans laquelle vous configurez les paramètres du lancement rapide EC2.
5. La case Launch template (Modèle de lancement) permet d'effectuer une recherche filtrée des modèles de lancement de votre compte dans la région actuelle qui correspondent au texte que vous avez saisi. Spécifiez la totalité ou une partie du nom ou de l'ID du modèle de lancement dans la case pour afficher la liste des modèles de lancement correspondants. Par exemple, si vous saisissez `fast` dans la case, Amazon EC2 trouve tous les modèles de lancement de votre compte dans la région actuelle dont le nom contient « `fast` ».

Pour créer votre modèle de lancement, vous pouvez choisir Create launch template (Créer un modèle de lancement).

6. Lorsque vous sélectionnez un modèle de lancement, Amazon EC2 affiche la version par défaut de ce modèle dans la case Source template version (Version du modèle source). Pour

spécifier une version différente, mettez en évidence la version par défaut pour la remplacer et saisissez le numéro de version souhaité dans la case.

7. Une fois les modifications terminées, choisissez Save changes (Enregistrer les modifications).

AWS CLI, API

Pour spécifier le modèle de lancement pour EC2 Fast Launch à partir du AWS CLI, spécifiez le nom ou l'ID du modèle de lancement dans le `--launch-template` paramètre lorsque vous exécutez la commande [enable-fast-launch](#) dans le AWS CLI

Pour spécifier le modèle de lancement pour EC2 Fast Launch dans une demande d'API, spécifiez le nom ou l'ID du modèle de lancement dans le `LaunchTemplate` paramètre lorsque vous appelez l'action [EnableFastLaunch](#) API.

Pour en savoir plus sur l'utilisation des modèles de lancement EC2, consultez [Lancer une instance à partir d'un modèle de lancement](#).

Créez une image personnalisée avec EC2 Fast Launch activé

Amazon EC2 EC2 Fast Launch s'intègre à EC2 Image Builder pour vous aider à créer des images personnalisées avec EC2 Fast Launch activé. Pour plus d'informations, consultez [Créer des paramètres de distribution pour une AMI Windows pour laquelle le lancement rapide EC2 est activé \(AWS CLI\)](#) dans le Guide de l'utilisateur d'EC2 Image Builder.

Afficher les AMI avec EC2 Fast Launch activé

Vous pouvez utiliser la commande [describe-fast-launch-images](#) dans l' AWS CLI PowerShell applet de commande [Get-EC2FastLaunchImage](#) Tools for pour obtenir des informations sur les AMI sur lesquelles EC2 Fast Launch est activé.

Amazon EC2 fournit les détails suivants pour chaque AMI Windows qui est retourné dans les résultats :

- ID d'image pour une AMI avec EC2 Fast Launch activé.
- Le type de ressource utilisé pour l'approvisionnement préalable de l'AMI Windows associée. Valeur prise en charge : snapshot.
- La configuration des instantanés, qui est un groupe de paramètres configurant le provisionnement préalable de l'AMI Windows associée à l'aide d'instantanés.

- Des informations sur le modèle de lancement, y compris l'ID, le nom et la version du modèle de lancement utilisé par l'AMI associée lorsqu'elle lance des instances Windows à partir d'instantanés provisionnés préalablement.
- Le nombre maximum d'instances qui peuvent être lancées en même temps pour créer des ressources.
- L'ID du propriétaire de l'AMI associée. Ce champ n'est pas renseigné pour les AMI qui sont partagées avec vous.
- État actuel d'EC2 Fast Launch pour l'AMI associée. Les valeurs prises en charge incluent : `enabling` | `enabling-failed` | `enabled` | `enabled-failed` | `disabling` | `disabling-failed`.

Note

Vous pouvez également consulter l'état actuel affiché dans la page `Manage image optimization` (Gérer l'optimisation des images) de la console EC2, comme `Image optimization state` (État d'optimisation de l'image).

- La raison pour laquelle le lancement rapide d'EC2 pour l'AMI associée est passé à l'état actuel.
- Heure à laquelle EC2 Fast Launch pour l'AMI associée est passée à l'état actuel.

Choisissez l'onglet qui correspond à votre environnement de ligne de commande :

AWS CLI

La `describe-fast-launch-images` commande appelle l'opération d'[DescribeFastLaunchImagesAPI](#) Amazon EC2.

Syntaxe :

```
aws ec2 describe-fast-launch-images \  
  --image-ids <value> \ (optional) \  
  --filters <value> \ (optional) \  
  --dry-run | --no-dry-run \ (optional) \  
  --cli-input-json <value> \ (optional) \  
  --starting-token <value> \ (optional) \  
  --page-size <value> \ (optional) \  
  --max-items <value> \ (optional) \  
  --generate-cli-skeleton <value> \ (optional)
```

Exemple :

L'exemple [describe-fast-launch-images](#) suivant décrit les détails de chacune des AMI du compte qui sont configurées pour EC2 Fast Launch. Dans cet exemple, une seule AMI du compte est configurée pour le lancement rapide d'EC2.

```
aws ec2 describe-fast-launch-images
```

Sortie :

```
{
  "FastLaunchImages": [
    {
      "ImageId": "ami-01234567890abcdef",
      "ResourceType": "snapshot",
      "SnapshotConfiguration": {},
      "LaunchTemplate": {
        "LaunchTemplateId": "lt-01234567890abcdef",
        "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
        "Version": "1"
      },
      "MaxParallelLaunches": 6,
      "OwnerId": "0123456789123",
      "State": "enabled",
      "StateTransitionReason": "Client.UserInitiated",
      "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
    }
  ]
}
```

Tools for PowerShell

L'Get-EC2FastLaunchImageapplet de commande appelle l'opération d'API Amazon [DescribeFastLaunchImages](#)EC2.

Syntaxe :

```
Get-EC2FastLaunchImage
-Filter <Filter[]>
-ImageId <String[]>
-MaxResult <Int32>
-NextToken <String>
```

```
-Select <String>  
-NoAutoIteration <SwitchParameter>
```

Exemple :

L'[Get-EC2FastLaunchImage](#) exemple suivant décrit les détails de chacune des AMI du compte configurées pour EC2 Fast Launch. Dans cet exemple, une seule AMI du compte est configurée pour le lancement rapide d'EC2.

```
Get-EC2FastLaunchImage -ImageId ami-01234567890abcdef
```

Sortie :

```
ImageId           : ami-01234567890abcdef  
LaunchTemplate    :  
  Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse  
MaxParallelLaunches : 6  
OwnerId           : 0123456789123  
ResourceType      : snapshot  
SnapshotConfiguration :  
State             : enabled  
StateTransitionReason : Client.UserInitiated  
StateTransitionTime : 2/25/2022 12:54:43 PM
```

Gérez les coûts des ressources avec EC2 Fast Launch

La configuration des AMI Windows pour EC2 Fast Launch est gratuite. Toutefois, lorsque vous activez EC2 Fast Launch pour une AMI Windows Amazon EC2, la tarification standard s'applique aux ressources AWS sous-jacentes utilisées par Amazon EC2 pour préparer et stocker les instantanés préprovisionnés. Vous pouvez configurer des balises de répartition des coûts pour vous aider à suivre et à gérer les coûts associés aux ressources EC2 Fast Launch. Pour plus d'informations sur la configuration des balises de répartition des coûts, consultez [Suivez les coûts de lancement rapide d'EC2 sur votre facture](#).

L'exemple suivant montre comment les coûts associés aux coûts des snapshots EC2 Fast Launch peuvent être répartis.

Exemple de scénario : la société AtoZ Example possède une AMI Windows avec un volume racine EBS de 50 Gio. Ils activent EC2 Fast Launch pour leur AMI et fixent le nombre de ressources cible

à cinq. Au cours d'un mois, l'utilisation d'EC2 Fast Launch pour leur AMI leur coûte environ 5\$, et la répartition des coûts est la suivante :

1. Lorsqu'AtoZ Example active le lancement rapide d'EC2, Amazon EC2 lance cinq petites instances. Chaque instance passe par les étapes de lancement de Windows Sysprep et OOBE, en redémarrant si nécessaire. Cela prend plusieurs minutes pour chaque instance (le temps peut varier, en fonction de l'activité de la région ou de la zone de disponibilité (AZ) et de la taille de l'AMI).

Coûts

- Coûts d'exécution des instances (ou durée d'exécution minimale, le cas échéant) : cinq instances
 - Coûts des volumes : cinq volumes racine EBS
2. Lorsque le processus de pré-provisionnement est terminé, Amazon EC2 prend un instantané de l'instance, qu'il stocke dans Amazon S3. Les instantanés sont généralement stockés pendant 4 à 8 heures avant d'être consommés par un lancement. Dans ce cas, le coût est d'environ 0,02 à 0,05 USD par instantané.

Coûts

- Stockage d'instantanés (Amazon S3) : cinq instantanés
3. Une fois qu'Amazon EC2 a pris l'instantané, il arrête l'instance. À ce stade, l'instance ne génère plus de coûts. Cependant, les coûts des volumes EBS continuent de s'accumuler.

Coûts

- Volumes EBS : les coûts continuent pour les volumes racine EBS associés.

Note

Les coûts présentés ici sont uniquement à des fins de démonstration. Vos coûts varieront en fonction de la configuration de votre AMI et de votre plan tarifaire.

Suivez les coûts de lancement rapide d'EC2 sur votre facture

Les étiquettes de répartition des coûts peuvent vous aider à organiser votre AWS facture afin de refléter les coûts associés à EC2 Fast Launch. Vous pouvez utiliser la balise suivante qu'Amazon

EC2 ajoute aux ressources qu'il crée lorsqu'il prépare et stocke des instantanés préprovisionnés pour EC2 Fast Launch :

Clé de balise : CreatedBy, Valeur : EC2 Fast Launch

Après avoir activé la balise dans la console de Billing and Cost Management et configuré votre rapport de facturation détaillé, la colonne `user:CreatedBy` apparaît sur le rapport. La colonne inclut les valeurs de tous les services. Toutefois, si vous téléchargez le fichier CSV, vous pouvez importer les données dans une feuille de calcul et appliquer un filtre pour EC2 Fast Launch dans la valeur. Ces informations apparaissent également AWS Cost and Usage Report lorsque le tag est activé.

Étape 1 : Activer les balises de répartition des coûts définies par l'utilisateur

Pour inclure les balises de ressources dans vos rapports sur les coûts, vous devez tout d'abord activer la balise dans la console Billing and Cost Management. Pour plus d'informations, consultez [Activation des balises de répartition des coûts définies par l'utilisateur](#) dans le Guide de l'utilisateur AWS Billing and Cost Management .

 Note

L'activation peut prendre jusqu'à 24 heures.

Étape 2 : Définition d'un rapport sur les coûts

Si vous avez déjà configuré un rapport sur les coûts, une colonne correspondant à votre balise s'affichera lors de la prochaine exécution du rapport, une fois l'activation terminée. Pour configurer les rapports sur les coûts pour la première fois, sélectionnez l'une des options suivantes.

- Veuillez consulter la rubrique [Setting up a monthly cost allocation report](#) (Configuration du rapport de répartition des coûts mensuel) dans le Guide de l'utilisateur AWS Billing and Cost Management .
- Veuillez consulter la rubrique [Creating Cost and Usage Reports](#) (Créer des rapports de coûts et d'utilisation) dans le Guide de l'utilisateur AWS Cost and Usage Report .

 Note

Cela peut prendre jusqu'à 24 heures pour commencer AWS à envoyer des rapports à votre compartiment S3.

Vous pouvez configurer EC2 Fast Launch pour les AMI Windows dont vous êtes propriétaire ou les AMI partagées avec vous à partir de la console Amazon EC2, de l'API, des kits SDK ec2 ou des [CloudFormation](#) commandes du. AWS CLI Les sections suivantes décrivent les étapes de configuration de la console Amazon EC2 et. AWS CLI

Vous pouvez également créer des AMI Windows personnalisées configurées pour EC2 Fast Launch avec EC2 Image Builder. Pour plus d'informations, voir [Créer des paramètres de distribution pour une AMI Windows avec EC2 Fast Launch activé \(AWS CLI\)](#).

Lancement rapide du moniteur EC2

Cette section explique comment surveiller les AMI Amazon EC2 Windows Server de votre compte sur lesquelles EC2 Fast Launch est activé.

Surveillez les changements d'état de lancement rapide d'EC2 avec EventBridge

Lorsque l'état change pour une AMI Windows avec EC2 Fast Launch activé, Amazon EC2 génère EC2 Fast Launch State-change Notification un événement. Amazon EC2 envoie ensuite l'événement de changement d'état à Amazon EventBridge (anciennement Amazon CloudWatch Events).

Vous pouvez créer des EventBridge règles qui déclenchent une ou plusieurs actions en réponse à l'événement de changement d'état. Par exemple, vous pouvez créer une EventBridge règle qui détecte le moment où EC2 Fast Launch est activé et exécute les actions suivantes :

- Envoie un message à une rubrique Amazon SNS pour informer ses abonnés.
- Appelle une fonction Lambda qui effectue une action.
- Envoie les données de changement d'état à Amazon Data Firehose à des fins d'analyse.

Pour plus d'informations, consultez [la section Création de EventBridge règles Amazon qui réagissent aux événements](#) dans le guide de EventBridge l'utilisateur Amazon.

Événements de changement d'état

La fonctionnalité EC2 Fast Launch émet au mieux des événements de changement d'état au format JSON. Amazon EC2 envoie les événements à quasiment EventBridge en temps réel. Cette section décrit les champs d'événement et présente un exemple de format d'événement.

EC2 Fast Launch State-change Notification

imageId

Identifie l'AMI avec le changement d'état EC2 Fast Launch.

resourceType

Type de ressource à utiliser pour l'allocation préalable. Valeur prise en charge : snapshot. La valeur par défaut est snapshot.

state

État actuel de la fonctionnalité de lancement rapide EC2 pour l'AMI spécifiée. Les valeurs valides sont notamment les suivantes :

- **activation** : vous avez activé la fonctionnalité EC2 Fast Launch pour l'AMI, et Amazon EC2 a commencé à créer des instantanés pour le processus de pré-provisionnement.
- **enabling-failed** : une erreur s'est produite et le processus de préprovisionnement a échoué la première fois que vous avez activé le lancement rapide EC2 pour une AMI. Cela peut se produire à tout moment pendant le processus d'allocation préalable.
- **activé** — La fonction EC2 Fast Launch est activée. L'état change `enabled` dès qu'Amazon EC2 crée le premier instantané préprovisionné pour une AMI EC2 Fast Launch nouvellement activée. Si l'AMI était déjà activée et passe à nouveau par l'allocation préalable, le changement d'état se produit immédiatement.
- **enabled-failed** : cet état ne s'applique que si ce n'est pas la première fois que votre AMI EC2 Fast Launch passe par le processus de préprovisionnement. Cela peut se produire si la fonctionnalité EC2 Fast Launch est désactivée puis réactivée ultérieurement, ou s'il y a un changement de configuration ou une autre erreur une fois le pré-provisionnement terminé pour la première fois.
- **désactivation** : le propriétaire de l'AMI a désactivé la fonction de lancement rapide EC2 pour l'AMI et Amazon EC2 a lancé le processus de nettoyage.
- **désactivé** — La fonction de lancement rapide d'EC2 est désactivée. L'état passe à `disabled` dès qu'Amazon EC2 termine le processus de nettoyage.
- **disabling-failed** : un problème est survenu et a entraîné l'échec du processus de nettoyage. Cela signifie que certains instantanés préalloués peuvent encore être conservés dans le compte.

état TransitionReason

La raison pour laquelle l'état a changé pour l'AMI EC2 Fast Launch.

Note

Tous les champs de ce message d'événement sont requis.

L'exemple suivant montre une AMI EC2 Fast Launch récemment activée qui a lancé la première instance pour démarrer le processus de préprovisionnement. À ce stade, l'état est `enabling`. Une fois qu'Amazon EC2 a créé le premier instantané préalloué, l'état passe à `enabled`.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EC2 Fast Launch State-change Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2022-08-31T20:30:12Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
  ],
  "detail": {
    "imageId": "ami-123456789012",
    "resourceType": "snapshot",
    "state": "enabling",
    "stateTransitionReason": "Client.UserInitiated"
  }
}
```

Surveillez les métriques de lancement rapide d'EC2 avec CloudWatch

Les AMI Amazon EC2 avec EC2 Fast Launch activé envoient des métriques à Amazon CloudWatch. Vous pouvez utiliser l'API AWS Management Console, l'AWS CLI, ou une API pour répertorier les métriques auxquelles EC2 Fast Launch envoie CloudWatch. L'espace de noms AWS/EC2 inclut les métriques EC2 Fast Launch suivantes :

Métrique	Description
<code>NumberOfAvailableFastLaunchSnapshots</code>	Nombre de snapshots préprovisionnés disponibles par AMI compatible avec EC2 Fast Launch.

Métrique	Description
NumberOfInstancesFastLancé	Nombre d'instances par AMI activée par EC2 Fast Launch qui ont été lancées à partir de snapshots préprovisionnés.
NumberOfInstancesNotFastLaunched	Le nombre d'instances par AMI activée par EC2 Fast Launch a entraîné un démarrage à froid en raison de l'absence de snapshots préprovisionnés disponibles au moment du lancement.
FastLaunchSnapshotUsedToRefillStartTime	L'horodatage auquel Amazon EC2 lançait une nouvelle image à partir d'un lancement rapide EC2 a permis à l'AMI de créer un autre instantané après l'utilisation d'un instantané existant.
FastLaunchSnapshotCreationHeure	Mesure le temps nécessaire à Amazon EC2 pour lancer une instance et créer un instantané pour une AMI compatible avec EC2 Fast Launch.

Rôle lié au service pour EC2 Fast Launch

Amazon EC2 utilise des rôles liés à un service pour les autorisations requises pour appeler d'autres Services AWS en votre nom. Un rôle lié à un service est un type unique de rôle IAM directement lié à un Service AWS. Les rôles liés à un service constituent un moyen sécurisé de déléguer des autorisations, Services AWS car seul le service lié peut assumer un rôle lié au service. Pour plus d'informations sur la façon dont Amazon EC2 utilise les rôles IAM, y compris les rôles liés à un service, consultez [Rôles IAM pour Amazon EC2](#).

Amazon EC2 utilise le rôle lié à un service intitulé `AWSServiceRoleForEC2FastLaunch` pour créer et gérer un ensemble d'instantanés approvisionnés préalablement qui réduisent le temps nécessaire au lancement d'instances à partir de votre AMI Windows.

Vous n'avez pas besoin de créer manuellement ce rôle lié à un service. Lorsque vous commencez à utiliser EC2 Fast Launch pour votre AMI, Amazon EC2 crée le rôle lié au service pour vous, s'il n'existe pas déjà.

Note

Si le rôle lié au service est supprimé de votre compte, vous pouvez activer EC2 Fast Launch pour qu'une autre AMI Windows puisse recréer le rôle dans votre compte. Vous pouvez également désactiver EC2 Fast Launch pour votre AMI actuelle, puis le réactiver. Toutefois, lorsque la fonctionnalité est désactivée, votre AMI commence à utiliser le processus de lancement standard pour toutes les nouvelles instances, tandis qu'Amazon EC2 supprime tous vos instantanés pré-approvisionnés. Une fois que tous les instantanés préprovisionnés ont disparu, vous pouvez réactiver l'utilisation d'EC2 Fast Launch pour votre AMI.

Amazon EC2 ne vous autorise pas à modifier le rôle lié à un service `AWSServiceRoleForEC2FastLaunch`. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de toutes les ressources connexes. Cela protège les ressources Amazon EC2 associées à votre AMI Amazon EC2 Windows Server avec EC2 Fast Launch activé, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Amazon EC2 prend en charge le rôle lié au service EC2 Fast Launch dans toutes les régions où le service Amazon EC2 est disponible. Pour plus d'informations, consultez [Régions](#).

Autorisations octroyées par `AWSServiceRoleForEC2FastLaunch`

Amazon EC2 utilise la politique gérée `EC2FastLaunchServiceRolePolicy` pour réaliser les actions suivantes :

- `cloudwatch:PutMetricData`— Publiez les données métriques associées à EC2 Fast Launch dans l'espace de noms Amazon EC2.
- `ec2:CreateLaunchTemplate`— Créez un modèle de lancement pour votre AMI Amazon EC2 Windows Server avec EC2 Fast Launch activé.
- `ec2:CreateSnapshot`— Créez des instantanés préconfigurés pour votre AMI Amazon EC2 Windows Server avec EC2 Fast Launch activé.

- `ec2:CreateTags`— Créez des balises pour les ressources associées au lancement et au préprovisionnement d'instances Windows pour votre AMI Amazon EC2 Windows Server avec EC2 Fast Launch activé.
- `ec2:DeleteSnapshots`— Supprimez tous les instantanés préprovisionnés associés si le lancement rapide EC2 est désactivé pour une AMI précédemment activée.
- `ec2:DescribeImages` : décrire les images de toutes les ressources.
- `ec2:DescribeInstanceAttribute` : décrire les attributs d'instance de toutes les ressources.
- `ec2:DescribeInstanceState` : décrire l'état de l'instance de toutes les ressources.
- `ec2:DescribeInstances` : décrire les instances de toutes les ressources.
- `ec2:DescribeInstanceTypeOfferings` : décrire les offres de type d'instance de toutes les ressources.
- `ec2:DescribeLaunchTemplates` : décrire les modèles de lancement de toutes les ressources.
- `ec2:DescribeLaunchTemplateVersions` : décrire les versions du modèle de lancement de toutes les ressources.
- `ec2:DescribeSnapshots` : décrire les ressources des instantanés de toutes les ressources.
- `ec2:DescribeSubnets` : décrire les sous-réseaux de toutes les ressources.
- `ec2:RunInstances`— Lancez des instances depuis une AMI Amazon EC2 Windows Server avec EC2 Fast Launch activé, afin d'effectuer les étapes de provisionnement.
- `ec2:StopInstances`— Arrêtez les instances lancées depuis une AMI Amazon EC2 Windows Server avec EC2 Fast Launch activé, afin de créer des instantanés préprovisionnés.
- `ec2:TerminateInstances`— Mettez fin à une instance qui a été lancée à partir d'une AMI Amazon EC2 Windows Server avec EC2 Fast Launch activé, après avoir créé le snapshot préprovisionné à partir de celle-ci.
- `iam:PassRole` : autorise le rôle lié à un service `AWSServiceRoleForEC2FastLaunch` à lancer des instances en votre nom à l'aide du profil d'instance de votre modèle de lancement.

Pour plus d'informations sur l'utilisation des politiques gérées avec Amazon EC2, consultez [AWS politiques gérées pour Amazon EC2](#).

Accéder aux clés gérées par le client en vue de leur utilisation avec les AMI chiffrées et les instantanés EBS

Prérequis

- Pour permettre à Amazon EC2 d'accéder à une AMI chiffrée en votre nom, vous devez avoir l'autorisation pour l'action `createGrant` dans la clé gérée par le client.

Lorsque vous activez EC2 Fast Launch pour une AMI chiffrée, Amazon EC2 garantit que `AWSServiceRoleForEC2FastLaunch` le rôle est autorisé à utiliser la clé gérée par le client pour accéder à votre AMI. Cette autorisation est nécessaire pour lancer des instances et créer des instantanés approvisionnés préalablement en votre nom.

Utiliser les accélérateurs Amazon Elastic Graphics sur les instances Windows

Important

Amazon Elastic Graphics a atteint sa fin de vie le 8 janvier 2024. Pour les charges de travail nécessitant une accélération graphique, nous vous recommandons d'utiliser des instances Amazon EC2 G4ad, G4dn ou G5.

Amazon Elastic Graphics offre une accélération graphique flexible, économique et haute performance pour vos instances Windows. Les accélérateurs Elastic Graphics sont disponibles en plusieurs tailles et constituent une alternative économique à l'utilisation de types d'instances graphiques GPU (tels que G3). Vous avez la possibilité de choisir un type d'instance qui répond aux exigences de calcul, de mémoire et de stockage de votre application. Ensuite, choisissez l'accélérateur pour votre instance qui répond aux exigences graphiques de votre charge de travail.

Elastic Graphics est adapté aux applications qui nécessitent un faible volume ou un volume intermittent d'accélération graphique supplémentaire, et qui s'appuient sur la prise en charge des cartes graphiques OpenGL. Pour bénéficier d'un accès direct et complet aux GPU attachés et utiliser les infrastructures de calcul parallèles DirectX, CUDA ou Open Computing Language (OpenCL), préférez une instance de type d'instance de calcul accéléré.

Table des matières

- [Principes de base d'un Elastic Graphics](#)

- [Tarification d'Elastic Graphics](#)
- [Limites Elastic Graphics](#)
- [Utiliser Elastic Graphics](#)
- [Maintenance des Elastic Graphics \(graphiques élastiques\)](#)
- [Utilisez CloudWatch des métriques pour surveiller Elastic Graphics](#)
- [Dépannage](#)

Principes de base d'un Elastic Graphics

Pour utiliser Elastic Graphics, lancez une instance Windows et spécifiez un type d'accélérateur pour l'instance lors du lancement. AWS trouve la capacité Elastic Graphics disponible et établit une connexion réseau entre votre instance et l'accélérateur Elastic Graphics.

Note

Les instances nues (Bare metal) ne sont pas prises en charge

Les accélérateurs Elastic Graphics sont disponibles dans les AWS régions suivantes : us-east-1, us-east-2, us-west-2, ap-northeast-1, ap-southeast-1, ap-southeast-2, eu-central-1, eu-west-1.

Les types d'instance suivants prennent en charge les accélérateurs Elastic Graphics :

- Usage général : M3, M4, M5, M5d, M5dn, M5n, T2, T3

Note

Seuls les modèles t2.medium, t3.medium et supérieurs sont pris en charge.

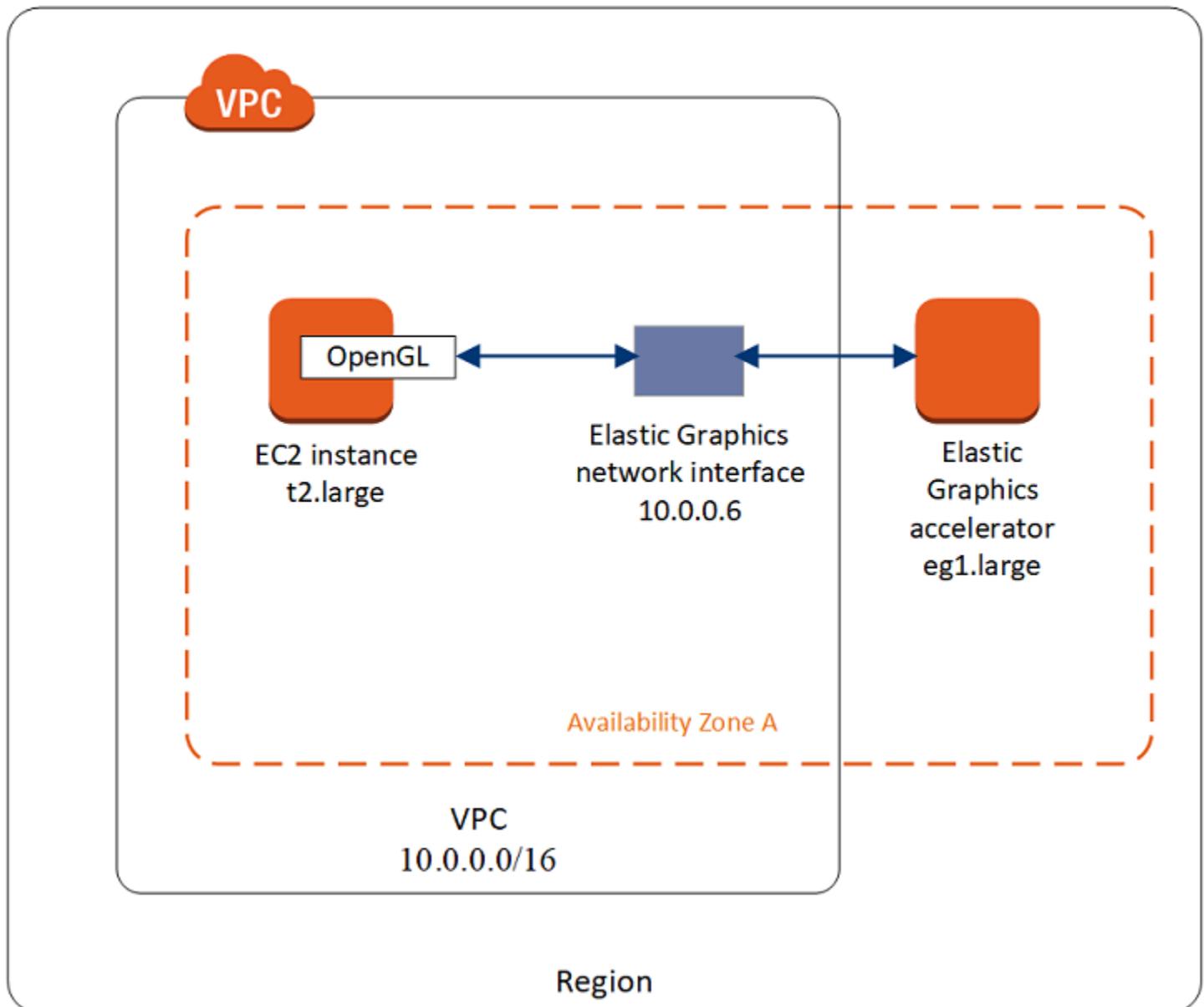
- Optimisées pour le calcul : C3, C4, C5, C5a, C5ad, C5d, C5n
- Optimisées pour la mémoire : R3, R4, R5, R5d, R5dn, R5n, X1, X1e, z1d
- Optimisées pour le stockage : D2, D3, D3en, H1, I3, I3en
- Calcul accéléré : P2, P3, P3dn

Les accélérateurs Elastic Graphics suivants sont disponibles. Vous pouvez attacher n'importe quel accélérateur Elastic Graphics aux différents types d'instance pris en charge.

Accélérateur Elastic Graphics	Mémoire graphique (Go)
eg1.medium	1
eg1.large	2
eg1.xlarge	4
eg1.2xlarge	8

Un accélérateur Elastic Graphics ne fait pas partie de la structure matérielle de votre instance. Il est au contraire attaché au réseau via une interface réseau connue sous le nom d'interface réseau Elastic Graphics. Lorsque vous lancez ou redémarrez une instance avec une accélération graphique, l'interface réseau Elastic Graphics est créée pour vous dans votre VPC.

L'interface réseau Elastic Graphics est créée dans les mêmes sous-réseau et VPC que votre instance, et est associée à une adresse IPv4 privée issue de ce sous-réseau. L'accélérateur attaché à votre instance Amazon EC2 provient d'un pool d'accélérateurs disponibles dans la même zone de disponibilité que votre instance.



Les accélérateurs Elastic Graphics prennent en charge les standards pour l'API OpenGL versions 4.3 et antérieures, qui peuvent être utilisés pour les applications par lot ou l'accélération graphique 3D. Une bibliothèque OpenGL optimisée pour Amazon sur votre instance détecte l'accélérateur attaché. Elle renvoie les appels de l'API OpenGL de votre instance vers l'accélérateur, qui traite ensuite les demandes et renvoie les résultats. Le trafic entre l'instance et l'accélérateur utilise la même bande passante que le trafic réseau de l'instance. Il est donc recommandé de disposer d'une bande passante réseau appropriée. Consultez votre fournisseur logiciel pour toute question concernant les versions et la conformité avec OpenGL.

Par défaut, le groupe de sécurité par défaut de votre VPC est associé à l'interface réseau Elastic Graphics. Le trafic réseau Elastic Graphics utilise le protocole TCP et le port 2007. Assurez-vous que le groupe de sécurité de votre instance le permette. Pour de plus amples informations, veuillez consulter [Configurer vos groupes de sécurité](#).

Tarification d'Elastic Graphics

Des frais vous sont facturés pour chaque seconde où un accélérateur Elastic Graphics est attaché à une instance dont l'état est `running` lorsque l'accélérateur est lui-même à l'état `Ok`. Aucuns frais ne vous sont facturés pour un accélérateur attaché à une instance dont l'état est `pending`, `stopping`, `stopped`, `shutting-down` ou `terminated`. De la même manière, aucuns frais ne vous sont facturés lorsque l'accélérateur est à l'état `Unknown` ou `Impaired`.

La tarification des accélérateurs est disponible uniquement pour les tarifs à la demande. Vous pouvez attacher un accélérateur à une instance réservée ou instance Spot. Toutefois, le prix à la demande de l'accélérateur s'applique.

Pour plus d'informations, consultez [Tarification Graphismes Amazon Elastic](#).

Limites Elastic Graphics

Avant d'utiliser les accélérateurs Elastic Graphics, tenez compte des restrictions suivantes :

- Vous ne pouvez attacher des accélérateurs qu'aux instances Windows avec Microsoft Windows Server 2012 R2 ou ultérieure. Les instances Linux ne sont pas prises en charge actuellement.
- Vous pouvez attacher un accélérateur à une instance à la fois.
- Vous ne pouvez attacher un accélérateur que pendant le lancement de l'instance. Vous ne pouvez pas attacher un accélérateur à une instance existante.
- Vous ne pouvez pas mettre en veille prolongée une instance avec un accélérateur attaché.
- Vous ne pouvez pas partager un accélérateur entre plusieurs instances.
- Vous ne pouvez pas détacher un accélérateur d'une instance ni le transférer à une autre instance. Si vous n'avez plus besoin d'un accélérateur, vous devez résilier votre instance. Pour modifier le type d'accélérateur, créez une AMI à partir de votre instance, résiliez cette dernière et lancez une nouvelle instance en spécifiant un autre accélérateur.
- Seules les versions 4.3 et antérieures de l'API OpenGL sont prises en charge. DirectX, CUDA et OpenCL ne sont pas pris en charge.
- L'accélérateur Elastic Graphics n'est ni visible ni accessible via le gestionnaire de périphériques de votre instance.

- Vous ne pouvez pas réserver ou planifier la capacité d'un accélérateur.

Utiliser Elastic Graphics

Important

Amazon Elastic Graphics a atteint sa fin de vie le 8 janvier 2024. Pour les charges de travail nécessitant une accélération graphique, nous vous recommandons d'utiliser des instances Amazon EC2 G4ad, G4dn ou G5.

Vous pouvez lancer une instance et l'associer à un accélérateur Elastic Graphics pendant la phase de lancement. Vous devez ensuite installer manuellement sur votre instance les bibliothèques nécessaires pour activer la communication avec l'accélérateur. Pour connaître les limitations, veuillez consulter [Limites Elastic Graphics](#).

Tâches

- [Configurer vos groupes de sécurité](#)
- [Lancer une instance avec un accélérateur Elastic Graphics](#)
- [Installer le logiciel requis pour Elastic Graphics](#)
- [Vérifier la fonctionnalité d'Elastic Graphics sur votre instance](#)
- [Afficher les informations d'Elastic Graphics](#)
- [Envoyer un commentaire](#)

Configurer vos groupes de sécurité

Les Elastic Graphics ont besoin d'un groupe de sécurité avec référence circulaire qui autorise tout le trafic entrant et sortant vers et depuis le groupe de sécurité proprement dit. Le groupe de sécurité doit comprendre les règles d'entrée et de sortie suivantes.

Entrant

Type	Protocole	Port	Source
Elastic Graphics	TCP	2007	L'ID du groupe de sécurité (son propre ID de ressource)

Sortant

Type	Protocole	Plage de ports	Destination
Elastic Graphics	TCP	2007	L'ID du groupe de sécurité (son propre ID de ressource)

Si vous utilisez la console Amazon EC2 pour lancer votre instance avec un accélérateur Elastic Graphics, vous pouvez autoriser l'assistant de lancement à créer automatiquement les règles de groupe de sécurité requises, ou sélectionner une sécurité que vous avez créée précédemment.

Si vous lancez votre instance à l'aide du SDK AWS CLI ou d'un SDK, vous devez spécifier un groupe de sécurité que vous avez créé précédemment.

Pour créer un groupe de sécurité pour Elastic Graphics

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité), puis Create security group (Créer un groupe de sécurité).
3. Dans la fenêtre Create security group (Créer un groupe de sécurité), procédez comme suit :
 - a. Pour Nom du groupe de sécurité, saisissez un nom descriptif pour le groupe de sécurité, tel que Elastic Graphics security group.
 - b. (Facultatif) Pour Description, saisissez une brève description du groupe de sécurité.
 - c. Pour VPC, sélectionnez le VPC dans lequel vous prévoyez d'utiliser Elastic Graphics.
 - d. Sélectionnez Create security group (Créer un groupe de sécurité).
4. Dans le volet de navigation, choisissez Security Groups (Groupes de sécurité), sélectionnez le groupe de sécurité que vous venez de créer, puis dans l'onglet Details (Détails), copiez l'ID du groupe de sécurité.
5. Dans l'onglet Inbound (Entrant), choisissez Edit (Modifier), puis procédez comme suit :
 - a. Choisissez Ajouter une règle.
 - b. Pour Type, choisissez Elastic Graphics.
 - c. Pour Source type (Type de source), choisissez Personnalisé.
 - d. Pour Source, collez l'ID de groupe de sécurité que vous avez copié précédemment.
 - e. Sélectionnez Enregistrer les règles.

6. Dans l'onglet Outbound rules (Règles sortantes), choisissez Edit outbound rules (Modifier les règles sortantes), puis procédez comme suit :
 - a. Choisissez Ajouter une règle.
 - b. Pour Type, choisissez Elastic Graphics.
 - c. Pour Destination type (Types de destination), choisissez Custom (Personnalisée).
 - d. Pour Destination, collez l'ID de groupe de sécurité que vous avez copié précédemment.
 - e. Sélectionnez Enregistrer les règles.

Pour plus d'informations, consultez [Groupes de sécurité Amazon EC2 pour vos instances EC2](#).

Lancer une instance avec un accélérateur Elastic Graphics

Vous pouvez associer un accélérateur Elastic Graphics à une instance au cours de son lancement. Le lancement peut échouer pour les raisons suivantes :

- Capacité de l'accélérateur Elastic Graphics insuffisante
- Limite d'accélérateurs Elastic Graphics dépassée dans la région
- Nombre d'adresses IPv4 privées dans votre VPC insuffisant pour créer une interface réseau pour l'accélérateur

Pour de plus amples informations, veuillez consulter [Limites Elastic Graphics](#).

Pour associer un accélérateur Elastic Graphics lors du lancement d'une instance (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sur le tableau de bord, choisissez Lancer une instance.
3. Sous Nom et balises, entrez une valeur pour Nom. Vous pouvez éventuellement choisir Ajouter des balises supplémentaires pour ajouter d'autres balises aux ressources associées à l'instance que vous lancez.
4. Sous Images de l'application et du système d'exploitation (Amazon Machine Image), sélectionnez une AMI Windows.
5. Pour Instance type (Type d'Instance), sélectionnez un type d'instance pris en charge. Pour plus d'informations, consultez [Principes de base d'un Elastic Graphics](#).
6. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou créez-en une.

7. À côté de Paramètres réseau, choisissez Modifier, puis spécifiez les paramètres réseau à utiliser pour votre instance.
 - a. Pour Réseau, sélectionnez un VPC pour votre instance.
 - b. Pour Sous-réseau, sélectionnez un sous-réseau dans lequel lancer votre instance.
 - c. Pour le pare-feu (groupes de sécurité), vous pouvez utiliser le groupe de sécurité que vous avez créé manuellement ou laisser la console créer un groupe de sécurité pour vous avec les règles entrantes et sortantes requises. [Configurer vos groupes de sécurité](#) Ajoutez des groupes de sécurité supplémentaires si nécessaire.
8. (Facultatif) Sous Configurer le stockage, configurez la taille de votre volume racine et ajoutez des volumes supplémentaires si nécessaire.
9. Développez la section Détails avancés.
10. Sous Détails avancés, pour Elastic GPU, sélectionnez un type d'accélérateur Elastic Graphics.
11. Dans le panneau Summary (Récapitulatif), sélectionnez Launch instance (Lancer l'instance).

Pour associer un accélérateur Elastic Graphics lors du lancement d'une instance (AWS CLI)

Vous pouvez utiliser la AWS CLI commande [run-instances](#) avec le paramètre suivant :

```
--elastic-gpu-specification Type=eg1.medium
```

Pour le paramètre `--security-group-ids`, vous devez inclure un groupe de sécurité qui contient les règles entrantes et sortantes requises. Pour plus d'informations, consultez [Configurer vos groupes de sécurité](#).

Pour associer un accélérateur Elastic Graphics lors du lancement de l'instance (Outils pour Windows PowerShell)

Utilisez la PowerShell commande [New-EC2Instance](#)Outils pour Windows.

Installer le logiciel requis pour Elastic Graphics

Si vous avez lancé votre instance à l'aide d'une AMI AWS Windows actuelle, le logiciel requis est automatiquement installé lors du premier démarrage. Si vous avez lancé votre instance à l'aide d'une AMI Windows qui n'installe pas automatiquement le logiciel requis, vous devez effectuer cette opération manuellement sur l'instance.

Pour installer le logiciel requis pour Elastic Graphics (si nécessaire)

1. Connectez-vous à l'instance.
2. Téléchargez le [programme d'installation Elastic Graphics](#) et ouvrez-le. Le gestionnaire d'installation se connecte au point de terminaison Elastic Graphics et télécharge la dernière version du logiciel requis.

Note

Si le lien de téléchargement ne fonctionne pas, essayez un autre navigateur ou copiez l'adresse du lien et collez-la dans un nouvel onglet de navigateur.

3. Redémarrez l'instance pour le vérifier.

Vérifier la fonctionnalité d'Elastic Graphics sur votre instance

Les packages Elastic Graphics installés sur votre instance incluent des outils qui vous permettent d'afficher le statut de l'accélérateur et de vérifier que les commandes OpenGL entre votre instance et l'accélérateur fonctionnent.

Si votre instance a été lancée avec une AMI sur laquelle les packages Elastic Graphics ne sont pas préinstallés, vous pouvez les télécharger et les installer vous-même. Pour plus d'informations, consultez [Installer le logiciel requis pour Elastic Graphics](#).

Vous pouvez utiliser l'une des méthodes suivantes afin de vérifier la fonctionnalité Elastic Graphics sur votre instance.

Note

Si le contrôleur d'état Elastic Graphics ou l'outil de ligne de commande renvoie un résultat inattendu, consultez la section [Résoudre les problèmes de statut Non sain](#).

Elastic Graphics status monitor

Vous pouvez utiliser l'outil de surveillance du statut pour afficher des informations sur le statut d'un accélérateur Elastic Graphics. Par défaut, cet outil est disponible dans la zone de notification de la barre des tâches de votre instance Windows. Il affiche le statut de l'accélérateur graphique. Les valeurs possibles sont les suivantes :

Sain

L'accélérateur Elastic Graphics est activé et sain.

Mise à jour en cours

Le statut de l'accélérateur Elastic Graphics est en cours de mise à jour. L'affichage du statut peut prendre quelques minutes.

Hors service

L'accélérateur Elastic Graphics est hors service. Pour obtenir des informations complémentaires sur l'erreur, choisissez [Read More](#) (En savoir plus).

Elastic Graphics command line tool

L'outil de ligne de commande Elastic Graphics, `egcli.exe`, permet de vérifier le statut de l'accélérateur. Si l'accélérateur rencontre un problème, l'outil renvoie un message d'erreur.

Pour lancer l'outil, ouvrez une invite de commande dans votre instance, puis exécutez la commande suivante :

```
C:\Program Files\Amazon\EC2ElasticGPUs\manager\egcli.exe
```

L'outil prend également en charge les paramètres suivants :

`--json, -j`

Indique si le message JSON doit être affiché. Les valeurs possibles sont `true` et `false`. La valeur par défaut est `true`.

`--imds, -i`

Indique si les métadonnées de l'instance pour la disponibilité de l'accélérateur doivent être vérifiées. Les valeurs possibles sont `true` et `false`. La valeur par défaut est `true`.

Voici un exemple de sortie. Le statut OK indique que l'accélérateur est activé et sain.

```
EG Infrastructure is available.  
Instance ID egpu-f6d94dfa66df4883b284e96db7397ee6  
Instance Type eg1.large  
EG Version 1.0.0.885 (Manager) / 1.0.0.95 (OpenGL Library) / 1.0.0.69 (OpenGL  
Redirector)
```

```
EG Status: Healthy
JSON Message:
{
  "version": "2016-11-30",
  "status": "OK"
}
```

Les valeurs possibles pour sont les suivantes status:

OK

L'accélérateur Elastic Graphics est activé et sain.

UPDATING

Le pilote Elastic Graphics est en cours de mise à jour.

NEEDS_REBOOT

Le pilote Elastic Graphics a été mis à jour et un redémarrage de l'instance Amazon EC2 est requis.

LOADING_DRIVER

Le pilote Elastic Graphics est en cours de chargement.

CONNECTING_EGPU

Le pilote Elastic Graphics est en train de vérifier la connectivité avec l'accélérateur Elastic Graphics.

ERROR_UPDATE_RETRY

Une erreur s'est produite pendant la mise à jour du pilote Elastic Graphics, une nouvelle tentative de mise à jour va bientôt être lancée.

ERROR_UPDATE

Une erreur irrécupérable s'est produite pendant la mise à jour du pilote Elastic Graphics.

ERROR_LOAD_DRIVER

Une erreur s'est produite lors du chargement du pilote Elastic Graphics.

ERROR_EGPU_CONNECTIVITY

L'accélérateur Elastic Graphics est irrécupérable.

Afficher les informations d'Elastic Graphics

Vous pouvez afficher des informations sur l'accélérateur Elastic Graphics attaché à votre instance.

Pour afficher les informations relatives à un accélérateur Elastic Graphics (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Instances, puis choisissez votre instance.
3. Sous l'onglet Détails, recherchez ID Elastic Graphics. Choisissez l'ID pour afficher les informations suivantes sur l'accélérateur Elastic Graphics :
 - État de l'attachement
 - Type
 - État de santé

Pour afficher les informations relatives à un accélérateur Elastic Graphics (AWS CLI)

Vous pouvez utiliser la commande [AWS CLI describe-elastic-gpus](#) :

```
aws ec2 describe-elastic-gpus
```

Vous pouvez utiliser la AWS CLI commande [describe-network-interfaces](#) et filtrer par ID de propriétaire pour afficher les informations relatives à l'interface réseau Elastic Graphics.

```
aws ec2 describe-network-interfaces --filters "Name=attachment.instance-owner-id,Values=amazon-elasticgpus"
```

Pour afficher des informations sur un accélérateur Elastic Graphics (Outils pour Windows PowerShell)

Utilisez les commandes suivantes :

- [Get-EC2ElasticGpu](#)
- [Get-EC2NetworkInterface](#)

Pour obtenir des informations sur un accélérateur Elastic Graphics à l'aide des métadonnées de l'instance

1. Connectez-vous à votre instance Windows qui utilise l'accélérateur Elastic Graphics.

2. Effectuez l'une des actions suivantes :

- À partir de PowerShell, utilisez l'applet de commande suivante :

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
```

- À partir de votre navigateur Web, collez l'URL suivante dans le champ d'adresse :

```
http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
```

Envoyer un commentaire

Vous pouvez envoyer des commentaires sur votre expérience avec Elastic Graphics pour que l'équipe puisse continuer à apporter des améliorations.

Pour envoyer des commentaires à l'aide de l'outil de surveillance du statut d'Elastic Graphics

1. Dans la zone de notification de la barre des tâches de votre instance Windows, ouvrez l'outil de surveillance du statut d'Elastic Graphics.
2. Dans l'angle inférieur gauche, choisissez Commentaire.
3. Saisissez votre commentaire et choisissez Soumettre.

Maintenance des Elastic Graphics (graphiques élastiques)

Important

Amazon Elastic Graphics a atteint sa fin de vie le 8 janvier 2024. Pour les charges de travail nécessitant une accélération graphique, nous vous recommandons d'utiliser des instances Amazon EC2 G4ad, G4dn ou G5.

AWS peut déterminer qu'un accélérateur Elastic Graphics est en mauvais état si :

- Une mise à jour de sécurité ou d'infrastructure est nécessaire
- Une mise à jour logicielle est nécessaire
- Il y a un problème avec l'hôte sous-jacent

Lorsqu'il est AWS déterminé qu'un accélérateur Elastic Graphics est en mauvais état, il planifie sa mise hors service. AWS vous informe de l'imminence du départ à la retraite de l'accélérateur et vous indique les mesures correctives que vous devez prendre.

Rubriques

- [Comment serai-je averti ?](#)
- [Que dois-je faire ?](#)
- [Que se passe-t-il lorsqu'un accélérateur atteint sa date de mise hors service ?](#)

Comment serai-je averti ?

Lorsque vous AWS planifiez le retrait d'un accélérateur Elastic Graphics, celui-ci envoie un avis de retrait de l'accélérateur à votre compte [AWS Health Dashboard](#). AWS envoie également un e-mail à l'adresse e-mail associée à votre AWS compte. Il s'agit de la même adresse e-mail que vous utilisez pour vous connecter à AWS Management Console.

Note

Si vous utilisez un compte e-mail que vous ne consultez pas régulièrement, utilisez le AWS Health Dashboard pour déterminer si l'un de vos accélérateurs Elastic Graphics doit être retiré. Vous pouvez également modifier les informations de contact de votre AWS compte sur la page des [paramètres du compte](#).

L'avis de mise hors service prévoit ce qui suit :

- ID de l'instance à laquelle l'accélérateur est attaché
- Informations sur le problème qui a un impact sur l'accélérateur
- La date de mise hors service de l'accélérateur
- Les mesures correctives que vous devez prendre

Que dois-je faire ?

Lorsque vous êtes averti que votre accélérateur Elastic Graphics est programmé pour une mise hors service, vous devez [Arrêter et démarrer l'instance](#) auquel l'accélérateur est attaché pour l'ancien accélérateur non sain à remplacer par un nouvel accélérateur sain.

Nous vous recommandons de fermer les applications graphiques exécutées sur l'instance avant d'arrêter et de redémarrer l'instance.

⚠ Important

Si vous n'arrêtez pas et ne démarrez pas votre instance avant la date de mise hors service planifiée, l'accélérateur associé à votre instance est automatiquement arrêté, ce qui peut entraîner l'arrêt de fonctionnement de vos applications.

Vous devez arrêter et démarrer l'instance. Le redémarrage de l'instance ne remplacera pas l'accélérateur non sain par un accélérateur sain.

Que se passe-t-il lorsqu'un accélérateur atteint sa date de mise hors service ?

Lorsqu'un accélérateur Elastic Graphics défaillant atteint sa date de mise hors service prévue, il est AWS définitivement arrêté. Pour recevoir un remplacement de votre accélérateur non sain, avant ou après la date de mise hors service, vous devez arrêter et démarrer l'instance à laquelle l'accélérateur est attaché.

Si vous n'arrêtez pas et ne démarrez pas votre instance avant la date de mise hors service planifiée, l'accélérateur associé à votre instance est automatiquement arrêté, ce qui peut entraîner l'arrêt de fonctionnement de vos applications.

Utilisez CloudWatch des métriques pour surveiller Elastic Graphics

⚠ Important

Amazon Elastic Graphics a atteint sa fin de vie le 8 janvier 2024. Pour les charges de travail nécessitant une accélération graphique, nous vous recommandons d'utiliser des instances Amazon EC2 G4ad, G4dn ou G5.

Vous pouvez surveiller votre accélérateur Elastic Graphics à l'aide d'Amazon CloudWatch, qui collecte des statistiques sur les performances de votre accélérateur. Ces statistiques sont enregistrées pour une durée de deux semaines. Vous pouvez, par conséquent, accéder aux informations historiques et mieux comprendre la façon dont votre service fonctionne.

Par défaut, les accélérateurs Elastic Graphics envoient des données métriques par intervalles CloudWatch de 5 minutes.

Pour plus d'informations sur Amazon CloudWatch, consultez le [guide de CloudWatch l'utilisateur Amazon](#).

Métriques pour un Elastic Graphics

L'espace de noms AWS/ElasticGPUs inclut les métriques suivantes pour Elastic Graphics.

Métrique	Description
Défaillance du ConnectivityCheck GPU	Indique si la connectivité avec l'accélérateur Elastic Graphics est active ou si elle a échoué. La valeur zéro (0) indique que la connexion est active. La valeur un (1) indique qu'elle a échoué. Unités : nombre
Défaillance du HealthCheck GPU	Indique si l'état de l'accélérateur Elastic Graphics a été vérifié au cours de la minute précédente. La valeur zéro (0) indique que le contrôle de statut a réussi. La valeur un (1) indique un échec du contrôle du statut. Unités : nombre
GPU MemoryUtilization	Mémoire du GPU utilisée. Unités : Mio

Dimensions d'Elastic Graphics

Vous pouvez filtrer les données de métriques de vos accélérateurs Elastic Graphics à l'aide des dimensions suivantes.

Dimension	Description
EGPUId	Filtre les données en fonction de l'accélérateur Elastic Graphics.
InstanceId	Filtre les données en fonction de l'instance à laquelle l'accélérateur Elastic Graphics est attaché.

Afficher CloudWatch les statistiques pour Elastic Graphics

Les métriques sont d'abord regroupées par espaces de noms de service, puis par dimensions prises en charge. Vous pouvez utiliser les procédures suivantes pour afficher les métriques de vos accélérateurs Elastic Graphics.

Pour consulter les métriques d'Elastic Graphics à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Si nécessaire, changez la région. À partir de la barre de navigation, sélectionnez la région dans laquelle réside votre accélérateur Elastic Graphics. Pour plus d'informations, consultez [Régions et points de terminaison](#).
3. Dans le volet de navigation, sélectionnez Metrics (Métriques).
4. Pour All metrics (Toutes les métriques), sélectionnez Elastic Graphics, Elastic Graphics Metrics (Métriques Elastic Graphics).

Pour afficher les métriques Elastic Graphics (AWS CLI)

Utilisez la commande [list-metrics](#) suivante :

```
aws cloudwatch list-metrics --namespace "AWS/ElasticGPUs"
```

Créez des CloudWatch alarmes pour surveiller Elastic Graphics

Vous pouvez créer une CloudWatch alarme qui envoie un message Amazon SNS lorsque l'alarme change d'état. Une alarme surveille une seule métrique sur une durée définie et envoie une notification à une rubrique Amazon SNS en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de durées.

Vous pouvez, par exemple, créer une alarme qui surveille l'état d'un accélérateur Elastic Graphics et envoie une notification lorsque que la vérification de l'état de l'accélérateur graphique échoue à trois reprises consécutives pendant cinq minutes.

Pour créer une alarme pour le statut d'intégrité d'un accélérateur Elastic Graphics

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le volet de navigation, choisissez Alarmes, puis Créer une alarme.
3. Choisissez Select metric (Sélectionner une métrique), Elastic Graphics, Elastic Graphics Metrics (Métriques Elastic Graphics).

4. Sélectionnez la métrique GPU HealthCheck Failed, puis sélectionnez Select metric.
5. Configurez l'alarme comme suit :
 - a. Sous Alarm details (Détails de l'alarme), saisissez un nom et une description pour votre alarme. Pour Whenever (Quand), choisissez \geq et entrez 1.
 - b. Pour Actions, sélectionnez une liste de notifications existante ou choisissez Nouvelle liste.
 - c. Sélectionnez Créer une alarme.

Dépannage

Important

Amazon Elastic Graphics a atteint sa fin de vie le 8 janvier 2024. Pour les charges de travail nécessitant une accélération graphique, nous vous recommandons d'utiliser des instances Amazon EC2 G4ad, G4dn ou G5.

Vous trouverez ci-dessous des erreurs et des étapes de dépannage courantes.

Table des matières

- [Examiner les problèmes de performance des applications](#)
 - [Problèmes de performance du rendu OpenGL](#)
 - [Problèmes de performance d'accès à distance](#)
- [Résoudre les problèmes de statut Non sain](#)
 - [Vérifier la configuration des instances](#)
 - [Arrêter et démarrer l'instance](#)
 - [Vérifier les composants installés](#)
 - [Vérifier les journaux Elastic Graphics](#)
- [Pourquoi est-ce que je vois plusieurs ENI ?](#)

Examiner les problèmes de performance des applications

Elastic Graphics utilise le réseau de l'instance pour envoyer des commandes OpenGL à une carte graphique attachée à distance. Par ailleurs, un bureau exécutant une application OpenGL avec un accélérateur Elastic Graphics est généralement accessible via technologie d'accès à distance. Il est

important de distinguer les problèmes de performance liés au rendu OpenGL ou à la technologie d'accès distant au bureau.

Problèmes de performance du rendu OpenGL

Les performances de rendu OpenGL sont déterminées par le nombre de commandes OpenGL et d'images générées sur l'instance à distance.

Les performances de rendu peuvent varier selon les facteurs suivants :

- Performances de l'accélérateur Elastic Graphics
- Performances réseau
- Performances de l'UC
- Modèle de rendu, complexité du scénario
- Comportement de l'application OpenGL

Un moyen facile d'évaluer les performances est d'afficher le nombre d'images rendues sur l'instance à distance. Les accélérateurs Elastic Graphics affichent un maximum de 25 i/s sur l'instance à distance pour obtenir la meilleure qualité perçue tout en réduisant l'utilisation réseau.

Pour afficher le nombre d'images produites

1. Ouvrez le fichier suivant dans un éditeur de texte. Si le fichier n'existe pas, créez-le.

```
C:\Program Files\Amazon\EC2ElasticGPUs\conf\eg.conf
```

2. Identifiez la section [Application] ou ajoutez-le s'il n'est pas présent, puis ajoutez le paramètre de configuration suivant :

```
[Application]  
show_fps=1
```

3. Redémarrez l'application, puis revérifiez les images par seconde.

Si le nombre d'i/s atteint entre 15 et 25 lors de la mise à jour de la scène rendue, cela signifie que l'accélérateur Elastic Graphics fonctionne au maximum. Tout autre problème de performances rencontré est probablement lié à l'accès à distance au bureau de l'instance. Si tel est le cas, consultez la section relative aux problèmes de performance d'accès à distance.

Si le nombre d'images par seconde est inférieur à 15, vous pouvez essayer de suivre la procédure ci-dessous :

- Améliorez les performances de l'accélérateur Elastic Graphics en sélectionnant un type d'accélérateur graphique plus puissant.
- Améliorez les performances réseau globales en suivant les trois conseils ci-dessous :
 - Vérifiez le volume de bande passante entrante et sortante en direction et en provenance du point de terminaison de l'accélérateur Elastic Graphics. Le point de terminaison de l'accélérateur Elastic Graphics peut être récupéré à l'aide de la PowerShell commande suivante :

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/meta-data/elastic-gpus/associations/[ELASTICGPU_ID]).content
```

- Le trafic réseau entre l'instance et le point de terminaison de l'accélérateur Elastic Graphics est lié au volume de commandes que l'application OpenGL produit.
- Le trafic réseau entre le point de terminaison de l'accélérateur Elastic Graphics et l'instance est lié au nombre d'images générées par l'accélérateur graphique.
- Si le volume d'utilisation du réseau atteint le débit réseau maximal des instances, essayez d'utiliser une instance proposant un débit réseau supérieur.
- Amélioration des performances de l'UC :
 - Les applications peuvent exiger un volume important de ressources d'UC en plus de celles dont a besoin l'accélérateur Elastic Graphics. Si le gestionnaire de tâches Windows signale qu'un grand volume de ressources d'UC est utilisé, essayez d'utiliser une instance offrant une plus grande puissance d'UC.

Problèmes de performance d'accès à distance

Une instance associée à un accélérateur Elastic Graphics est accessible avec différentes technologies d'accès à distance. Les performances et la qualité peuvent varier selon différents facteurs :

- Technologie d'accès à distance
- Performances de l'instance
- Performance du client
- Latence réseau et bande passante entre le client et l'instance

Choix possibles pour le protocole d'accès à distance :

- Connexion Bureau à distance Microsoft
- NICE DCV
- VNC

Pour plus d'informations sur l'optimisation, reportez-vous au protocole correspondant.

Résoudre les problèmes de statut Non sain

Si l'accélérateur Elastic Graphics n'est pas sain, utilisez les étapes suivantes pour résoudre le problème.

Vérifier la configuration des instances

Si l'outil de ligne de commande Elastic Graphics, `egcli.exe`, renvoie des informations semblables à ce qui suit, assurez-vous que votre [groupe de sécurité est correctement configuré](#) et que vous avez lancé l'instance avec Instance Metadata Service activé.

```
EG Version 1.0.7.4240 (Manager) / N/A (OpenGL Library) / N/A (OpenGL Redirector)
EG Status: Out Of Service
Something prevented the EG Infrastructure to work properly.
```

Arrêter et démarrer l'instance

Si votre accélérateur Elastic Graphics n'est pas sain, il est recommandé d'arrêter puis de redémarrer l'instance. Pour de plus amples informations, veuillez consulter [Arrêtez et démarrez manuellement vos instances](#).

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instance sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

Vérifier les composants installés

Ouvrez le Panneau de configuration Windows et vérifiez que les composants suivants sont installés :

- Gestionnaire Amazon Elastic Graphics
- Bibliothèque OpenGL Amazon Elastic Graphics
- Redirecteur OpenGL d'Elastic GPUs Amazon EC2

Si l'un de ces composants est absent, vous devez l'installer manuellement. Pour de plus amples informations, veuillez consulter [Installer le logiciel requis pour Elastic Graphics](#).

Vérifier les journaux Elastic Graphics

Ouvrez l'Observateur d'événements Windows, développez la section Journaux des applications et des services, puis recherchez d'éventuelles erreurs dans les journaux d'événements suivants :

- EC2ElasticGPUs
- EC2ElasticGPUs GUI

Pourquoi est-ce que je vois plusieurs ENI ?

Lorsque vous appelez [StartInstances](#) une instance EC2 avec un accélérateur Elastic Graphics, une nouvelle Elastic Network Interface (ENI) est créée sur l'instance pour permettre l'envoi de commandes OpenGL à la carte graphique connectée à distance.

Si vous appelez [StartInstances](#) plusieurs fois en peu de temps (quelques secondes ou moins) sur la même instance EC2, une nouvelle interface réseau est créée à chaque appel. Cependant :

- une seule interface réseau est utilisée par l'accélérateur Elastic Graphics ;
- les interfaces réseau supplémentaires ne sont pas facturées et sont automatiquement publiées sous 24 heures.

Installation de WSL sur votre instance Windows

Windows Subsystem for Linux (WSL) est en téléchargement gratuit que vous pouvez installer sur votre instance Windows. En installant WSL, vous pouvez exécuter des outils de ligne de commande Linux natifs directement sur votre instance Windows et utiliser les outils Linux pour l'écriture de scripts, parallèlement à votre bureau Windows traditionnel. Vous pouvez facilement passer de Linux à Windows sur une seule instance Windows, ce qui peut s'avérer utile dans un environnement de développement.

Pour plus d'informations sur WSL, consultez la [documentation du sous-système Windows pour Linux](#) sur le site web de Microsoft Build.

Limites

- WSL est disponible en deux versions : WSL 1 et WSL 2.
 - Pour les instances EC2 `.metal`, vous pouvez installer WSL 1 ou WSL 2.
 - Pour les instances EC2 virtualisées, vous devez installer WSL 1.
- Pour les systèmes d'exploitation Windows Server, WSL ne peut être installé que sur des instances exécutant ce qui suit :
 - Windows Server 2019
 - Windows Server 2022

Installation de WSL

Les instructions suivantes installent WSL sur une instance EC2 exécutant Windows Server 2022. Pour les instructions d'installation de WSL sur une instance EC2 exécutant Windows Server 2019, consultez [Installer WSL sur les versions antérieures de Windows Server](#) sur le site web de Microsoft. Après avoir suivi ces instructions, vous pouvez utiliser l'étape 3 des instructions ci-dessous pour configurer WSL afin d'utiliser WSL 1.

Installez WSL 1

1. Pour installer WSL, exécutez la commande d'installation standard suivante sur votre instance EC2, mais veillez à activer WSL 1 en incluant `--enable-wsl1`. Par défaut, WSL 2 est également installé. Si votre instance a été lancée à l'aide d'un type d'instance virtualisée, vous devez effectuer l'étape 3 de cette procédure pour définir la version sur WSL 1.

```
ws1 --install --enable-wsl1 --no-launch
```

2. Redémarrez votre instance EC2.

```
shutdown -r -t 20
```

3. Pour configurer WSL afin d'utiliser WSL 1, exécutez la commande suivante dans votre instance. Pour plus d'informations sur la configuration de la version WSL, consultez la section [Étapes d'installation manuelle pour les anciennes versions de WSL](#) sur le site Web de Microsoft Build.

```
wsl --set-default-version 1
```

4. Installez la distribution par défaut.

```
wsl --install
```

Installez WSL 2

- Pour installer WSL, exécutez la commande d'installation standard suivante sur votre instance EC2. Par défaut, WSL 2 est également installé. Si vous installez WSL sur une instance `.metal`, c'est la seule étape à effectuer.

```
wsl --install
```

Pour plus d'informations, consultez [Installer Linux sur Windows avec WSL](#) sur le site web de Microsoft Build.

Mettre à niveau une instance Amazon EC2 Windows vers une nouvelle version de Windows Server

Il existe deux méthodes pour mettre à niveau une version antérieure de Windows Server exécutée sur une instance : la mise à niveau sur place et la migration (également appelée side-by-side mise à niveau). Une mise à niveau sur place met à niveau les fichiers de système d'exploitation tout en gardant intacts vos paramètres et fichiers personnels. Une migration implique la capture de paramètres, de configurations et de données et leur portage vers un système d'exploitation sur une nouvelle instance Amazon EC2.

Microsoft recommande traditionnellement de migrer vers une version plus récente de Windows Server plutôt que d'effectuer une mise à niveau. La migration entraîne moins d'erreurs ou de problèmes de mise à niveau, mais peut être plus longue qu'une mise à niveau sur place, car elle nécessite la mise en service d'une nouvelle instance, la planification et des applications de port et le réglage des paramètres de configurations sur la nouvelle instance. Une mise à niveau sur place peut être plus rapide, mais les incompatibilités logicielles peuvent entraîner des erreurs.

Table des matières

- [Effectuez une mise à niveau sur place sur votre instance Windows](#)
- [Effectuez une mise à niveau automatique sur votre instance Windows](#)
- [Migrer une instance Windows vers un type d'instance de génération actuelle](#)
- [Assistant de replateforme Windows vers Linux pour les bases de données Microsoft SQL Server](#)
- [Résoudre les problèmes liés à une mise à niveau sur une instance Windows](#)

Effectuez une mise à niveau sur place sur votre instance Windows

Avant d'effectuer une mise à niveau sur place, vous devez déterminer quels pilotes réseau sont exécutés par l'instance. Les pilotes réseau PV vous permettent d'accéder à votre instance à l'aide des services Bureau à distance. Les instances utilisent des pilotes AWS PV, Intel Network Adapter ou Enhanced Networking. Pour plus d'informations, consultez [Pilotes de virtualisation paravirtuelle pour les instances Windows](#).

Avant de commencer une mise à niveau sur place

Exécutez les tâches suivantes et prenez note des renseignements importants suivants avant de démarrer la mise à niveau sur place.

- Lisez la documentation Microsoft pour comprendre la configuration requise de la mise à niveau, les problèmes connus et les restrictions. Consultez également les instructions officielles de la mise à niveau.
 - [Upgrade Options for Windows Server 2012](#)
 - [Upgrade Options for Windows Server 2012 R2](#)
 - [Upgrade and conversion options for Windows Server 2016](#)
 - [Upgrade and conversion options for Windows Server 2019](#)
 - [Upgrade and conversion options for Windows Server 2022](#)
 - [Upgrade Center Windows Server](#)
- Nous recommandons d'effectuer une mise à niveau du système d'exploitation sur les instances avec au moins 2 vCPU et 4 Go de RAM. Si nécessaire, vous pouvez changer l'instance à une taille plus grande du même type (t2.small à t2.large, par exemple), effectuer la mise à niveau, puis la redimensionner à la taille originale. Si vous devez conserver la taille de l'instance, vous pouvez suivre la progression à l'aide de [Capture d'écran de console d'instance](#). Pour plus d'informations, consultez [Modifier le type d'instance](#).

- Vérifiez que le volume racine de votre instance Windows dispose d'un espace disque suffisant. Le processus de l'installation Windows peut ne pas vous avertir en cas d'espace disque insuffisant. Pour obtenir plus d'informations sur l'espace disque requis pour mettre à niveau un système d'exploitation spécifique, consultez la documentation Microsoft. Si le volume ne dispose pas d'un espace suffisant, celui-ci peut être étendu. Pour plus d'informations, consultez [Amazon EBS Elastic Volumes](#) dans le guide de l'utilisateur Amazon EBS.
- Déterminez le chemin de votre mise à niveau. Vous devez mettre à niveau le système d'exploitation sur la même architecture. Par exemple, vous devez mettre à niveau un système 32 bits vers un système 32 bits. Windows Server 2008 R2 et les versions ultérieures sont compatibles avec des systèmes 64 bits uniquement.
- Désactivez les logiciels anti-virus et anti-espion, ainsi que les pare-feu. Ces types de logiciels peuvent créer des conflits avec le processus de mise à niveau. Une fois la mise à niveau terminée, réactivez les logiciels anti-virus et anti-espion, ainsi que les pare-feu.
- Mettre à jour les derniers pilotes comme décrit dans [Migrer une instance Windows vers un type d'instance de génération actuelle](#).
- Le service UpgradeHelperService prend uniquement en charge les instances exécutant des pilotes PV Citrix. Si l'instance exécute des pilotes Red Hat, vous devez d'abord les [mettre à niveau](#) manuellement.

Mettez à niveau une instance sur place avec le AWS PV, l'adaptateur réseau Intel ou les pilotes réseau améliorés

Utilisez la procédure suivante pour mettre à niveau une instance Windows Server utilisant des pilotes PV AWS , de carte réseau Intel ou de la mise en réseau améliorée.

Pour exécuter une mise à niveau sur place

1. Créez une AMI du système que vous prévoyez de mettre à niveau à des fins de sauvegarde ou de test. Vous pouvez ensuite exécuter la mise à niveau sur la copie pour simuler un environnement de test. Si la mise à niveau réussit, vous pouvez basculer le trafic vers cette instance avec une interruption courte. Si la mise à niveau échoue, vous pouvez restaurer la sauvegarde. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).
2. Assurez-vous que votre instance Windows Server utilise les derniers pilotes réseau.
 - a. Pour mettre à jour votre pilote AWS PV, voir [Mise à niveau des pilotes PV sur les instances Windows](#).

- b. Pour mettre à jour votre pilote ENA, consultez [Installation du pilote Elastic Network Adapter \(ENA\)](#).
 - c. Pour mettre à jour vos pilotes Intel, voir [Activez une mise en réseau améliorée avec l'interface Intel 82599 VF sur vos instances EC2](#)
3. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
 4. Dans le panneau de navigation, choisissez Instances. Recherchez l'instance. Notez l'ID et la zone de disponibilité de l'instance. Vous aurez besoin de ces informations ultérieurement lors de cette procédure.
 5. Si vous effectuez la mise à niveau depuis Windows Server 2012 ou 2012 R2 vers Windows Server 2016, 2019 ou 2022, procédez comme suit sur votre instance avant de continuer :
 - a. Désinstallez le service EC2Config. Pour plus d'informations, consultez [Arrêter, redémarrer, supprimer ou désinstaller EC2Config](#).
 - b. Installez EC2Launch v1 ou l'agent EC2Launch v2. Pour plus d'informations, consultez [Configurer une instance Windows à l'aide d'EC2Launch](#) et [Configurer une instance Windows à l'aide d'EC2Launch v2](#).
 - c. Installez l'agent AWS Systems Manager SSM. Pour plus d'informations, consultez [Utilisation de SSM Agent](#) dans le Guide de l'utilisateur AWS Systems Manager .
 6. Créez un volume à partir d'un instantané du média d'installation de Windows Server.
 - a. Dans le panneau de navigation, sous Elastic Block Store, sélectionnez Instantanés.
 - b. Dans la barre Filtre, choisissez Instantanés publics.
 - c. Dans la barre de recherche, spécifiez les filtres suivants :
 - Choisissez Alias du propriétaire, puis =, puis Amazon.
 - Choisissez Description, puis commencez à taper **Windows**. Sélectionnez le filtre Windows qui correspond à l'architecture système et la préférence de langue vers lesquelles vous effectuez la mise à niveau. Par exemple, sélectionnez Windows 2019 English Installation Media pour mettre à niveau vers Windows Server 2019.
 - d. Cochez la case à côté de l'instantané correspondant à l'architecture du système et la langue préférée vers laquelle vous souhaitez effectuer la mise à niveau, puis sélectionnez Actions, Create volume from snapshot (Créer un volume à partir d'un instantané).
 - e. Dans la boîte de dialogue Create volume (Créer un volume), sélectionnez la zone de disponibilité correspondant à votre instance Windows, puis choisissez Create volume (Créer un volume).

7. Dans la bannière Successfully created volume vol-**1234567890example** (Exemple de volume vol-1234567890 créé avec succès) en haut de la page, choisissez l'ID du volume que vous venez de créer.
8. Sélectionnez Actions, puis Attach volume (Attacher un volume).
9. Sur la page Attach volume (Attacher un volume), pour l'Instance, sélectionnez l'ID d'instance de votre instance Windows, puis choisissez Attach volume (Attacher un volume).
10. Rendez le nouveau volume disponible pour utilisation en suivant les étapes décrites dans [Mettre un volume Amazon EBS à disposition pour utilisation](#).

 Important

Ne pas initialiser le disque car cela supprimerait les données existantes.

11. Sous Windows PowerShell, passez au nouveau lecteur de volume. Commencez la mise à niveau en ouvrant le volume du média d'installation que vous avez attaché à l'instance.
 - a. Si vous mettez à niveau vers Windows Server 2016 ou ultérieur, procédez comme suit :

```
.\setup.exe /auto upgrade /dynamicupdate disable
```

 Note

L'exécution du setup.exe avec l'option /dynamicupdate définie sur désactivée empêche Windows d'installer des mises à jour pendant le processus de mise à niveau de Windows Server, car l'installation de mises à jour pendant la mise à niveau peut provoquer des échecs. Vous pouvez installer les mises à jour avec Windows Update une fois la mise à niveau terminée.

Si vous mettez à niveau vers une version précédente de Windows Server, procédez comme suit :

```
Sources\setup.exe
```

- b. Sur la page Sélectionner le système d'exploitation à installer, sélectionnez le SKU d'installation complet correspondant à votre instance Windows Server, puis choisissez Suivant.

- c. Pour Quel type d'installation voulez-vous effectuer ?, choisissez Mise à niveau.
- d. Exécutez l'assistant.

La configuration de Windows Server copie et traite les fichiers. Quelques minutes plus tard, votre session des services Bureau à distance se ferme. Le délai de la mise à niveau dépend du nombre d'applications et de rôles de serveurs s'exécutant sur votre instance Windows Server. Le processus de mise à niveau peut prendre de 40 minutes à plusieurs heures. L'instance échoue au contrôle de statut 1 sur 2 pendant le processus de mise à niveau. Une fois la mise à niveau terminée, les deux contrôles de statut réussissent. Vous pouvez consulter le journal système pour connaître les résultats de la console ou utiliser CloudWatch les métriques Amazon relatives à l'activité du disque et du processeur afin de déterminer si la mise à niveau progresse.

Note

Si vous mettez à niveau vers Windows Server 2019, une fois la mise à niveau terminée, vous pouvez modifier manuellement l'arrière-plan du bureau pour supprimer le nom du système d'exploitation précédent si vous le souhaitez.

Si l'instance n'a pas validé les deux contrôles des statuts au bout de plusieurs heures, consultez [Résoudre les problèmes liés à une mise à niveau sur une instance Windows](#).

Tâches post-mise à niveau

1. Connectez-vous à l'instance pour initier une mise à niveau de .NET Framework et redémarrez le système quand vous y êtes invité.
2. Si vous ne l'avez pas déjà fait lors d'une étape précédente, installez l'agent EC2Launch v1 ou EC2Launch v2. Pour plus d'informations, consultez [Configurer une instance Windows à l'aide d'EC2Launch](#) et [Configurer une instance Windows à l'aide d'EC2Launch v2](#).
3. Si vous avez effectué la mise à niveau vers Windows Server 2012 R2, nous vous recommandons de mettre à niveau les pilotes PV vers des pilotes AWS PV. Si vous avez mis à niveau sur une instance Nitro, nous vous recommandons d'installer ou de mettre à niveau les pilotes NVMe et ENA. Pour plus d'informations, consultez [Windows Server 2012 R2](#), [Installez ou mettez à niveau les pilotes AWS NVMe à l'aide de PowerShell](#) ou [Activer les réseaux améliorés sur Windows](#).
4. Réactivez les logiciels anti-virus et anti-espion, ainsi que les pare-feu.

Effectuez une mise à niveau automatique sur votre instance Windows

Vous pouvez effectuer une mise à niveau automatique de vos instances Windows et SQL Server à l'AWS aide des runbooks AWS Systems Manager Automation.

Table des matières

- [Services connexes](#)
- [Options d'exécution](#)
- [Mettre à niveau Windows Server](#)
- [Mettre à niveau SQL Server](#)

Services connexes

Les AWS services suivants sont utilisés dans le processus de mise à niveau automatique :

- **AWS Systems Manager.** AWS Systems Manager est une interface puissante et unifiée permettant de gérer vos AWS ressources de manière centralisée. Pour plus d'informations, consultez le Guide de l'utilisateur [AWS Systems Manager](#).
- **AWS Systems Manager L'agent (agent SSM)** est un logiciel Amazon qui peut être installé et configuré sur une instance Amazon EC2, un serveur sur site ou une machine virtuelle (VM). SSM Agent permet à Systems Manager de mettre à jour, gérer et configurer ces ressources. L'agent traite les demandes du service Systems Manager dans le Cloud AWS , puis les exécute comme spécifié dans la demande. Pour plus d'informations, consultez [Utilisation de SSM Agent](#) dans le Guide de l'utilisateur AWS Systems Manager .
- **AWS Systems Manager Runbooks SSM.** Un runbook SSM définit les actions exécutées par Systems Manager sur vos instances gérées. Les runbooks SSM utilisent la notation JavaScript d'objet (JSON) ou YAML, et ils incluent des étapes et des paramètres que vous spécifiez. Cette rubrique utilise deux runbooks SSM Systems Manager d'automatisation. Pour plus d'informations, consultez [AWS Systems Manager Automation runbook reference](#) dans le Guide de l'utilisateur AWS Systems Manager .

Options d'exécution

Lorsque vous sélectionnez Automation (Automatisation) sur la console Systems Manager, choisissez Exécute (Exécuter). Après avoir sélectionné un document d'automatisation, vous êtes invité à choisir

une option d'exécution de l'automatisation. Choisissez parmi les options suivantes. Dans les étapes des chemins fournis dans cette rubrique, nous utilisons l'option d'exécution simple.

Exécution simple

Choisissez cette option si vous souhaitez mettre à jour une seule instance mais que vous ne voulez pas passer par chaque étape d'automatisation pour auditer les résultats. Cette option est décrite plus en détails dans les étapes de mise à niveau qui suivent.

Contrôle du débit

Choisissez cette option si vous souhaitez appliquer la mise à niveau à plusieurs instances. Définissez les paramètres suivants.

- Paramètre

Ce paramètre qui est également défini dans les paramètres Plusieurs comptes et plusieurs régions spécifie comment votre automatisation se ramifie.

- Cibles

Sélectionnez la cible à laquelle appliquer l'automatisation. Ce paramètre est également défini dans les paramètres Plusieurs comptes et plusieurs régions.

- Valeurs de paramètres

Utilisez les valeurs définies dans les paramètres du document d'automatisation.

- Groupe de ressources

Dans AWS, une ressource est une entité avec laquelle vous pouvez travailler. Les exemples incluent les instances Amazon EC2, les AWS CloudFormation stacks ou les buckets Amazon S3. Si vous travaillez avec plusieurs ressources, il peut être utile de les gérer en groupe plutôt que de passer d'un AWS service à l'autre pour chaque tâche. Dans certains cas, vous souhaitez gérer un grand nombre de ressources liées, comme les instances EC2 qui constituent une couche d'application. Dans ce cas, vous aurez probablement besoin d'exécuter des actions par lots simultanément sur ces ressources.

- Balises

Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Cette catégorisation est utile lorsque vous avez de nombreuses ressources du même type. Vous pouvez identifier rapidement une ressource spécifique à l'aide des balises attribuées.

- Contrôle du débit

Le contrôle du débit est également défini dans les paramètres Plusieurs comptes et plusieurs régions. Lorsque vous définissez des paramètres de contrôle du débit, vous spécifiez la part de votre flotte à laquelle appliquer l'automatisation, par nombre de cibles ou selon un pourcentage du flotte.

Plusieurs comptes et plusieurs régions

Il existe deux paramètres en plus des paramètres spécifiés sous Contrôle du débit qui sont également utilisés dans les paramètres Plusieurs comptes et plusieurs régions :

- Comptes et unités d'organisation (UO)

Spécifiez plusieurs comptes sur lesquels exécuter l'automatisation.

- Régions AWS

Spécifiez plusieurs Régions AWS endroits où vous souhaitez exécuter l'automatisation.

Exécution manuelle

Cette option est similaire à Exécution simple, mais elle vous permet d'exécuter l'automatisation étape par étape et d'auditer les résultats.

Mettre à niveau Windows Server

Le runbook [AWSEC2-CloneInstanceAndUpgradeWindows](#) crée une Amazon Machine Image (AMI) à partir d'une instance Windows Server dans votre compte et met à niveau cette AMI vers une version prise en charge de votre choix. Ce processus en plusieurs étapes peut prendre jusqu'à deux heures.

Deux AMI sont incluses dans le processus de mise à niveau automatisée :

- Instance en cours d'exécution actuelle. La première AMI est l'instance en cours d'exécution actuelle qui n'est pas mise à niveau. Cette AMI est utilisée pour lancer une autre instance afin d'exécuter la mise à niveau sur place. Lorsque le processus est terminé, cette AMI est supprimée de votre compte à moins que vous ne demandiez spécifiquement de conserver l'instance d'origine. Ce paramètre est traité par le paramètre `KeepPreUpgradeImageBackup` (la valeur par défaut est `false`, ce qui signifie que l'AMI est supprimée par défaut).

- AMI mise à niveau. Cette AMI est le résultat du processus d'automatisation.

Le résultat final est une AMI qui est l'instance mise à niveau de l'AMI.

Lorsque la mise à niveau est terminée, vous pouvez tester la fonctionnalité applicative en lançant la nouvelle AMI dans votre Amazon VPC. Après le test et avant de procéder à une autre mise à niveau, planifiez les temps d'arrêt de l'application avant de passer complètement à l'instance mise à niveau.

Prérequis

Afin d'automatiser votre mise à niveau de Windows Server avec le document AWS Systems Manager Automation, vous devez effectuer les tâches suivantes :

- Créez un rôle IAM avec les politiques IAM spécifiées pour autoriser Systems Manager à exécuter des tâches d'automatisation sur vos instances Amazon EC2 et vérifiez que vous répondez aux prérequis pour utiliser Systems Manager. Pour plus d'informations, consultez la section [Création d'un rôle pour déléguer des autorisations à un AWS service](#) dans le Guide de AWS Identity and Access Management l'utilisateur.
- [Sélectionnez l'option souhaitée pour l'exécution de l'automatisation](#). Les options d'exécution sont Exécution simple, Contrôle du débit, Plusieurs comptes et plusieurs régions et Exécution manuelle. Pour plus d'informations sur ces options, consultez [Options d'exécution](#).
- Vérifier que SSM Agent est installé sur votre instance. Pour plus d'informations, consultez [Installing and configuring SSM Agent on Amazon EC2 instances for Windows Server](#).
- Windows PowerShell 3.0 ou version ultérieure doit être installé sur votre instance.
- Pour les instances qui sont jointes à un domaine Microsoft Active Directory, nous vous recommandons de spécifier un SubnetId qui n'a pas de connectivité à vos contrôleurs de domaine afin d'éviter les conflits de noms d'hôte.
- Le sous-réseau de l'instance doit disposer d'une connectivité sortante à Internet, qui permet d'accéder Services AWS à Amazon S3 et de télécharger des correctifs depuis Microsoft. Cette exigence est satisfaite si le sous-réseau est un sous-réseau public et que l'instance possède une adresse IP publique, ou si le sous-réseau est un sous-réseau privé avec une route qui envoie le trafic Internet vers un périphérique NAT public.
- Cette automatisation fonctionne avec des instances exécutant Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 et Windows Server 2019.
- Vérifiez que l'instance a 20 Go d'espace disque libre dans le disque de démarrage.

- Si l'instance n'utilise pas de licence Windows fournie par AWS, spécifiez un ID de snapshot Amazon EBS qui inclut le support d'installation de Windows Server 2012 R2. Pour cela :
 1. Vérifiez que l'instance Amazon EC2 exécute Windows Server 2012 ou version ultérieure.
 2. Créez un volume Amazon EBS de 6 Go dans la même zone de disponibilité que celle où l'instance est en cours d'exécution. Attachez le volume à l'instance. Montez-la, par exemple, en tant que lecteur D.
 3. Cliquez avec le bouton droit de la souris sur le fichier ISO et montez-le sur une instance telle que le lecteur E.
 4. Copiez le contenu du fichier ISO depuis le lecteur E:\ vers le lecteur D:\.
 5. Créez un instantané Amazon EBS du volume de 6 Go comme à l'étape 2 ci-dessus.

Limitations de mise à niveau Windows Server

Cette procédure d'automatisation ne prend pas en charge la mise à niveau des contrôleurs de domaine Windows, des clusters ni des systèmes d'exploitation de bureau Windows. En outre, cette automatisation ne prend pas en charge les instances Amazon EC2 for Windows Server avec les rôles suivants installés :

- Hôte de session des services Bureau à distance (RDSH)
- Broker de connexion des services Bureau à distance (RDCB)
- Hôte de virtualisation des services Bureau à distance (RDVH)
- Accès web des services Bureau à distance (RDWA)

Étapes à suivre pour effectuer une mise à niveau automatisée de Windows Server

Suivez ces étapes pour mettre à niveau votre instance Windows Server à l'aide du runbook d'automatisation [CloneInstanceAndUpgradeWindows AWSEC 2-Windows](#).

1. Ouvrez Systems Manager depuis la Console de gestion AWS .
2. Dans le panneau de navigation de gauche, sous Change Management (Gestion des modifications), choisissez Automation (Automatisation).
3. Choisissez Execute automation (Exécuter l'automatisation).
4. Recherchez le document d'automatisation appelé AWSEC2-CloneInstanceAndUpgradeWindows.

5. Lorsque le nom du document apparaît, sélectionnez-le. Les détails du document apparaissent alors.
6. Choisissez `Execute automation` (Exécuter l'automatisation) afin de saisir les paramètres pour ce document. Laissez l'option `Exécution simple` sélectionnée en haut de la page.
7. Entrez les paramètres demandés en suivant les indications suivantes.

- `InstanceID`

Type : chaîne

(Obligatoire) Instance exécutant Windows Server 2008 R2, 2012 R2, 2016 ou 2019 avec SSM Agent installé.

- `InstanceProfile`.

Type : chaîne

(Obligatoire) Profil d'instance IAM. Il s'agit du rôle IAM utilisé pour effectuer l'automatisation de Systems Manager par rapport à l'instance AWS Amazon EC2 et aux AMI. Pour plus d'informations, consultez [Créer un profil d'instance IAM pour Systems Manager](#) dans le Guide de l'utilisateur AWS Systems Manager .

- `TargetWindowsVersion`

Type : chaîne

(Obligatoire) Sélectionnez la version cible de Windows.

- `SubnetId`

Type : chaîne

(Obligatoire) Il s'agit du sous-réseau pour le processus de mise à niveau et dans lequel l'instance EC2 source réside. Vérifiez que le sous-réseau dispose d'une connectivité sortante aux AWS services, notamment Amazon S3, ainsi qu'à Microsoft (afin de télécharger des correctifs).

- `KeepPreUpgradedBackUp`

Type : chaîne

(Facultatif) Si ce paramètre est défini sur `true`, l'automatisation conserve l'image créée depuis l'instance. Le paramètre par défaut est `false`.

- `RebootInstanceBeforeTakingImage`

Type : chaîne

(Facultatif) La valeur par défaut est `false` (pas de redémarrage). Si ce paramètre est défini sur `true`, Systems Manager redémarre l'instance avant de créer une AMI pour la mise à niveau.

8. Une fois que vous avez entré les paramètres, sélectionnez `Execute` (Exécuter). Lorsque l'automatisation commence, vous pouvez surveiller la progression de l'exécution.
9. Lorsque l'automatisation est terminée, vous verrez l'ID de l'AMI. Vous pouvez lancer l'AMI pour vérifier que le système d'exploitation Windows est mis à niveau.

Note

Il n'est nécessaire que l'automatisation exécute toutes les étapes. Les étapes sont conditionnelles en fonction du comportement de l'automatisation et de l'instance.

Systems Manager peut ignorer certaines étapes qui ne sont pas requises.

En outre, certaines étapes peuvent expirer. Systems Manager tente d'effectuer la mise à niveau et d'installer tous les derniers correctifs. Cependant, parfois, des correctifs expirent en fonction d'un paramètre de délai d'attente définissable pour l'étape donnée. Lorsque cela se produit, l'automatisation Systems Manager passe à l'étape suivante pour s'assurer que le système d'exploitation interne est mis à niveau vers la version de Windows Server cible.

10. Lorsque l'automatisation est terminée, vous pouvez lancer une instance Amazon EC2 à l'aide de l'ID d'AMI pour vérifier votre mise à niveau. Pour plus d'informations sur la création d'une instance Amazon EC2 à partir d'une AWS AMI, consultez [Comment lancer une instance EC2 à partir d'une AMI personnalisée ?](#)

Mettre à niveau SQL Server

Le script [AWSEC2-CloneInstanceAndUpgradeSQLServer](#) crée une AMI à partir d'une instance Amazon EC2 exécutant SQL Server dans votre compte, puis met à niveau l'AMI vers une version ultérieure de SQL Server. Ce processus en plusieurs étapes peut prendre jusqu'à deux heures.

Dans ce flux de travail, l'automatisation crée une AMI à partir de l'instance, puis lance la nouvelle AMI dans le sous-réseau que vous fournissez. L'automatisation exécute ensuite une mise à niveau sur

place de SQL Server. Une fois la mise à niveau terminée, l'automatisation crée une AMI avant de résilier l'instance mise à niveau.

Deux AMI sont incluses dans le processus de mise à niveau automatisée :

- Instance en cours d'exécution actuelle. La première AMI est l'instance en cours d'exécution actuelle qui n'est pas mise à niveau. Cette AMI est utilisée pour lancer une autre instance afin d'exécuter la mise à niveau sur place. Lorsque le processus est terminé, cette AMI est supprimée de votre compte à moins que vous ne demandiez spécifiquement de conserver l'instance d'origine. Ce paramètre est traité par le paramètre `KeepPreUpgradeImageBackUp` (la valeur par défaut est `false`, ce qui signifie que l'AMI est supprimée par défaut).
- AMI mise à niveau. Cette AMI est le résultat du processus d'automatisation.

Le résultat final est une AMI qui est l'instance mise à niveau de l'AMI.

Lorsque la mise à niveau est terminée, vous pouvez tester la fonctionnalité applicative en lançant la nouvelle AMI dans votre Amazon VPC. Après le test et avant de procéder à une autre mise à niveau, planifiez les temps d'arrêt de l'application avant de passer complètement à l'instance mise à niveau.

Prérequis

Afin d'automatiser votre mise à niveau de SQL Server avec le document AWS Systems Manager Automation, vous devez effectuer les tâches suivantes :

- Créez un rôle IAM avec les politiques IAM spécifiées pour autoriser Systems Manager à exécuter des tâches d'automatisation sur vos instances Amazon EC2 et vérifiez que vous répondez aux prérequis pour utiliser Systems Manager. Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur AWS Identity and Access Management .
- [Sélectionnez l'option souhaitée pour l'exécution de l'automatisation](#). Les options d'exécution sont Exécution simple, Contrôle du débit, Plusieurs comptes et plusieurs régions et Exécution manuelle. Pour plus d'informations sur ces options, consultez [Options d'exécution](#).
- L'instance Amazon EC2 doit utiliser Windows Server 2008 R2 ou version ultérieure et SQL Server 2008 ou version ultérieure.
- Vérifier que SSM Agent est installé sur votre instance. Pour plus d'informations, consultez [Utilisation de l'agent SSM sur les instances Amazon EC2 pour Windows Server](#).
- Vérifiez que l'instance dispose d'un espace disque suffisant :

- Si vous effectuez une mise à niveau de Windows Server 2008 R2 vers 2012 R2, ou de Windows Server 2012 R2 vers un système d'exploitation plus récent, vérifiez que vous disposez de 20 Go d'espace disque libre sur le disque de démarrage de l'instance.
- Si vous effectuez une mise à niveau de Windows Server 2008 R2 vers 2016 ou version ultérieure, vérifiez que l'instance dispose de 40 Go d'espace disque libre sur le disque de démarrage de l'instance.
- Pour les instances qui utilisent une version SQL Server avec apport de sa propre licence (BYOL), les prérequis supplémentaires suivants s'appliquent :
 - Fournissez un ID d'instantané Amazon EBS qui inclut le support d'installation de SQL Server. Pour cela :
 1. Vérifiez que l'instance Amazon EC2 exécute Windows Server 2008 R2 ou version ultérieure.
 2. Créez un volume Amazon EBS de 6 Go dans la même zone de disponibilité que celle où l'instance est en cours d'exécution. Attachez le volume à l'instance. Montez-la, par exemple, en tant que lecteur D.
 3. Cliquez avec le bouton droit de la souris sur le fichier ISO et montez-le sur une instance telle que le lecteur E.
 4. Copiez le contenu du fichier ISO depuis le lecteur E:\ vers le lecteur D:\.
 5. Créez un instantané Amazon EBS du volume de 6 Go comme à l'étape 2.

Limitations de mise à niveau automatisée SQL Server

Les limitations suivantes s'appliquent lors de l'utilisation du runbook

[AWSECCloneInstanceAndUpgrade2-SQLServer](#) pour effectuer une mise à niveau automatique :

- La mise à niveau peut uniquement être effectuée sur un serveur SQL à l'aide de l'authentification Windows.
- Vérifiez qu'il n'y a pas de correctifs et mises à jour de sécurité en attente sur les instances. Ouvrez le Panneau de configuration, puis choisissez Rechercher les mises à jour.
- Les déploiements SQL Server HA et le mode de mise en miroir ne sont pas pris en charge.

Étapes à suivre pour effectuer une mise à niveau automatisée de SQL Server

Suivez ces étapes pour mettre à niveau votre SQL Server à l'aide du [AWSECrunbook d'automatisation CloneInstance AndUpgrade 2-SQLServer](#).

1. Si vous ne l'avez déjà fait, téléchargez le fichier .iso SQL Server 2016 et montez-le sur le serveur source.
2. Une fois le fichier .iso monté, copiez tous les fichiers de composant et placez-les sur un volume de votre choix.
3. Prenez un instantané Amazon EBS du volume et copiez l'ID de l'instantané dans un presse-papiers pour une utilisation ultérieure. Pour plus d'informations, consultez la section [Créer des instantanés Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.
4. Attachez un profil d'instance à l'instance source Amazon EC2. Cela permet à Systems Manager de communiquer avec l'instance EC2 et d'exécuter des commandes sur celle-ci après son ajout au AWS Systems Manager service. Pour cet exemple, nous avons nommé le rôle SSM-EC2-Profile-Role avec la stratégie AmazonSSMManagedInstanceCore attachée au rôle. Consultez [Créer un profil d'instance IAM pour Systems Manager](#) dans le Guide de l'utilisateur AWS Systems Manager .
5. Dans le volet de navigation de gauche de la AWS Systems Manager console, sélectionnez Managed Instances. Vérifiez que votre instance EC2 se trouve dans la liste des instances gérées. Si vous ne voyez votre instance après quelques minutes, consultez [Où sont mes instances ?](#) dans le Guide de l'utilisateur AWS Systems Manager .
6. Dans le panneau de navigation de gauche, sous Change Management (Gestion des modifications), choisissez Automation (Automatisation).
7. Choisissez Execute automation (Exécuter l'automatisation).
8. Recherchez le document d'automatisation appelé AWSEC2-CloneInstanceAndUpgradeSQLServer.
9. Choisissez le document SSM AWSEC2-CloneInstanceAndUpgradeSQLServer, puis Next (Suivant).
10. Assurez-vous que l'option Simple execution (Exécution simple) est sélectionnée.
11. Entrez les paramètres demandés en suivant les indications suivantes.
 - InstanceId

Type : chaîne

(Obligatoire) Instance exécutant Windows Server 2008 R2 (ou version ultérieure).
 - IamInstanceProfile

Type : chaîne

(Obligatoire) Profil d'instance IAM.

- `SQLServerSnapshotId`

Type : chaîne

(Obligatoire) ID d'instantané du support d'installation de SQL Server cible. Ce paramètre n'est pas requis pour les instances SQL Server comprenant une licence.

- `SubnetId`

Type : chaîne

(Obligatoire) Il s'agit du sous-réseau pour le processus de mise à niveau et dans lequel l'instance EC2 source réside. Vérifiez que le sous-réseau dispose d'une connectivité sortante aux AWS services, notamment Amazon S3, ainsi qu'à Microsoft (afin de télécharger des correctifs).

- `KeepPreUpgradedBackup`

Type : chaîne

(Facultatif) Si ce paramètre est défini sur `true`, l'automatisation conserve l'image créée depuis l'instance. Le paramètre par défaut est `false`.

- `RebootInstanceBeforeTakingImage`

Type : chaîne

(Facultatif) La valeur par défaut est `false` (pas de redémarrage). Si ce paramètre est défini sur `true`, Systems Manager redémarre l'instance avant de créer une AMI pour la mise à niveau.

- `TargetSQLVersion`

Type : chaîne

(Facultatif) Version SQL Server cible. L'argument par défaut est `2016`.

12. Une fois que vous avez entré les paramètres, sélectionnez **Execute** (Exécuter). Lorsque l'automatisation commence, vous pouvez surveiller la progression de l'exécution.
13. Lorsque le champ **Execution Status** (Statut d'exécution) affiche **Success** (Réussite), choisissez la liste **Outputs** (Sorties) pour afficher les informations de l'AMI. Vous pouvez utiliser l'ID d'AMI afin de lancer votre instance SQL Server pour le VPC de votre choix.

14. Ouvrez la console Amazon EC2. Dans le volet de navigation de gauche, choisissez AMI. Vous devez voir la nouvelle AMI.
15. Pour vérifier que la nouvelle version de SQL Server a été installée avec succès, sélectionnez la nouvelle AMI et choisissez Launch (Lancer).
16. Choisissez le type d'instance souhaité pour l'AMI, le VPC et le sous-réseau vers lesquels déployer et le stockage à utiliser. Comme vous lancez la nouvelle instance depuis une AMI, les volumes vous sont présentés comme option à inclure au sein de la nouvelle EC2 que vous lancez. Vous pouvez supprimer tout volume ou ajouter des volumes.
17. Ajoutez une balise pour vous aider à identifier votre instance.
18. Ajoutez le ou les groupes de sécurité à l'instance.
19. Choisissez Launch Instances.
20. Choisissez le nom de la balise pour l'instance et sélectionnez Connexion sous la liste déroulante Actions.
21. Vérifiez que la nouvelle version de SQL Server est le moteur de base de données sur la nouvelle instance.

Migrer une instance Windows vers un type d'instance de génération actuelle

Les AMI AWS Windows sont configurées avec les paramètres par défaut utilisés par le support d'installation Microsoft, avec quelques personnalisations. Les personnalisations incluent des pilotes et des configurations qui prennent en charge les types d'instances de dernière génération, qui sont des [instances basées sur le système AWS Nitro](#), telles qu'une M5 ou une C5.

Lors de la migration vers des instances basées sur Nitro, y compris des instances nues, nous vous recommandons de suivre les étapes décrites dans cette rubrique dans les cas suivants :

- Si vous lancez des instances à partir d'AMI Windows personnalisées
- Si vous lancez des instances à partir d'AMI Windows fournies par Amazon qui ont été créées avant août 2018

Pour plus d'informations, consultez le blog [Amazon EC2 Update — Additional Instance Types, Nitro System, and CPU Options](#).

Note

Les procédures de migration suivantes peuvent être effectuées sur Windows Server version 2008 R2 et les versions ultérieures. Pour migrer des instances Linux vers les types d'instances de dernière génération, consultez [the section called "Modifier le type d'instance"](#).

Table des matières

- [Partie 1 : Installation et mise à niveau des pilotes AWS PV](#)
- [Partie 2 : Installer et mettre à niveau l'ENA](#)
- [Partie 3 : mise à niveau des pilotes AWS NVMe](#)
- [Étape 4 : Mettre à jour les services EC2Config et EC2Launch](#)
- [Étape 5 : Installer le pilote du port série pour les instances nues](#)
- [Étape 6 : Mettre à jour les paramètres de gestion de l'alimentation](#)
- [Étape 7 : Mettre à jour les pilotes de puce Intel pour des nouveaux types d'instance](#)
- [\(Alternative\) Mettez à niveau les pilotes AWS PV, ENA et NVMe à l'aide de AWS Systems Manager](#)
- [Migrer une instance Windows d'un type d'instance Nitro vers un type d'instance Xen](#)

Note

Vous pouvez également utiliser le document d'automatisation `AWSSupport-UpgradeWindowsAWSDrivers` pour automatiser les procédures décrites dans la première, la deuxième et la troisième étape. Si vous choisissez d'utiliser la procédure automatisée, consultez [\(Alternative\) Mettez à niveau les pilotes AWS PV, ENA et NVMe à l'aide de AWS Systems Manager](#), puis continuez avec la quatrième et la cinquième étape.

Avant de commencer

Cette procédure suppose que vous exécutez actuellement un type d'instance Xen de génération précédente, tel qu'un M4 ou un C4, et que vous migrez vers une [instance basée](#) sur le système Nitro. AWS

Vous devez utiliser PowerShell la version 3.0 ou ultérieure pour effectuer correctement la mise à niveau.

Note

Lors de la migration vers la dernière génération d'instances, l'IP statique ou les paramètres réseau DNS personnalisés sur l'ENI existante peuvent être perdus, car l'instance devient, par défaut, un nouveau périphérique Enhanced Networking Adapter (ENA).

Avant de commencer à suivre les étapes de cette procédure, nous vous conseillons de créer une sauvegarde de l'instance. Dans la [console EC2](#), choisissez l'instance qui nécessite la migration, ouvrez le menu contextuel (clic droit) et sélectionnez État de l'instance, puis Arrêter.

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour préserver les données qui se trouvent sur les volumes de stockage d'instances, assurez-vous de les sauvegarder dans un stockage permanent.

Ouvrez le menu contextuel (clic droit) de l'instance dans la [console EC2](#), choisissez Image, puis Créer une image.

Note

Les parties 4 et 5 de ces instructions peuvent être terminées après avoir migré ou modifié le type d'instance vers la dernière génération. Toutefois, nous vous recommandons de les terminer avant de procéder à la migration si vous migrez spécifiquement vers un type d'instance bare metal.

Partie 1 : Installation et mise à niveau des pilotes AWS PV

Bien que les pilotes AWS PV ne soient pas utilisés dans le système Nitro, vous devez tout de même les mettre à niveau si vous utilisez des versions précédentes de Citrix PV ou AWS PV. Les pilotes PV AWS permettent de corriger des bogues présents dans des versions précédentes de pilotes, susceptibles de se manifester sur un système Nitro, ou si vous devez revenir à une instance Xen. À titre de bonne pratique, nous vous recommandons de toujours mettre à jour les derniers pilotes pour les instances Windows activées AWS.

Utilisez la procédure suivante pour effectuer une mise à niveau sur place des pilotes AWS PV ou pour passer des pilotes PV Citrix aux pilotes AWS PV sous Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019. Pour plus d'informations, consultez [Mise à niveau des pilotes PV sur les instances Windows](#).

Pour mettre à niveau un contrôleur de domaine, consultez [Mettre à niveau un contrôleur de domaine \(mise à niveau AWS PV\)](#).

Pour effectuer une mise à niveau ou vers des pilotes AWS PV

1. Connectez-vous à l'instance à l'aide des services Bureau à distance et préparez l'instance à la mise à niveau. Mettez tous les disques non système hors ligne avant d'exécuter la mise à niveau. Si vous effectuez une mise à jour sur place des pilotes AWS PV, cette étape n'est pas obligatoire. Définissez les services non essentiels sur le start-up Manual (Manuel) dans la console Services.
2. [Téléchargez](#) le package de pilotes le plus récent sur l'instance.
3. Extrayez le contenu du dossier, puis exécutez `AWSPVDriverSetup.msi`.

Après avoir exécuté le MSI, l'instance redémarre automatiquement et met à niveau le pilote. L'instance ne sera peut-être pas disponible pendant 15 minutes.

Lorsque la mise à niveau est terminée et que l'instance réussit les deux vérifications de l'état dans la console Amazon EC2, connectez-vous à l'instance à l'aide des services Bureau à distance et vérifiez que le nouveau pilote a été installé. Dans le Gestionnaire de périphériques, sous Contrôleurs de stockage, recherchez Carte hôte AWS PV Storage. Vérifiez que la version du pilote est identique à la version la plus récente répertoriée dans l'historique des versions de pilote. Pour plus d'informations, consultez [AWS Historique du package de pilotes PV](#).

Partie 2 : Installer et mettre à niveau l'ENA

Effectuez une mise à niveau vers le pilote Elastic Network Adapter (ENA) le plus récent afin de garantir la prise en charge de toutes les fonctions du réseau. Si vous avez lancé votre instance et qu'elle n'a pas encore la mise en réseau améliorée activée, vous devez télécharger et installer le pilote de la carte réseau requis sur votre instance, puis définir l'attribut d'instance `enaSupport` pour activer la mise en réseau améliorée. Vous pouvez uniquement activer cet attribut sur les types d'instance pris en charge et seulement si le pilote ENA est installé. Pour plus d'informations, consultez [Activez une mise en réseau améliorée avec l'Elastic Network Adapter \(ENA\) sur vos instances EC2](#).

1. [Téléchargez](#) le pilote le plus récent sur l'instance.
2. Décompressez l'archive zip.
3. Installez le pilote en exécutant le `install.ps1` PowerShell script à partir du dossier extrait.

Note

Afin d'éviter les erreurs d'installation, exécutez le script `install.ps1` en tant qu'administrateur.

4. Vérifiez si `enaSupport` est activé pour votre AMI. Si ce n'est pas le cas, poursuivez à l'aide de la documentation disponible dans [Activez une mise en réseau améliorée avec l'Elastic Network Adapter \(ENA\) sur vos instances EC2](#).

Partie 3 : mise à niveau des pilotes AWS NVMe

AWS Les pilotes NVMe sont utilisés pour interagir avec Amazon EBS et les volumes de stockage d'instances SSD qui sont exposés sous forme de blocs NVMe dans le système Nitro pour de meilleures performances.

Important

Les instructions suivantes sont modifiées spécifiquement lorsque vous installez ou mettez à niveau AWS NVMe sur une instance de génération précédente dans le but de migrer l'instance vers le type d'instance de dernière génération.

1. [Téléchargez](#) le package de pilotes le plus récent sur l'instance.
2. Décompressez l'archive zip.
3. Installez le pilote en exécutant `dpinst.exe`.
4. Ouvrez une PowerShell session et exécutez la commande suivante :

```
PS C:\> start rundll32.exe sppnp.dll, Sysprep_Generalize_Pnp -wait
```

Note

Pour appliquer la commande, vous devez exécuter la PowerShell session en tant qu'administrateur. PowerShell les versions (x86) entraîneront une erreur.

Cette commande exécute uniquement Sysprep sur les pilotes de périphérique. Elle n'exécute pas la préparation Sysprep complète.

5. Pour Windows Server 2008 R2 et Windows Server 2012, arrêtez l'instance, remplacez le type d'instance par une instance de nouvelle génération et lancez-la. Passez ensuite à l'étape 4. Si vous redémarrez à nouveau l'instance sur un type d'instance de la génération précédente avant de migrer vers un type d'instance de nouvelle génération, elle ne démarrera pas. Pour les autres AMI Windows prises en charge, vous pouvez changer le type d'instance à tout moment après le Sysprep du périphérique.

Étape 4 : Mettre à jour les services EC2Config et EC2Launch

Pour les instances Windows, les derniers utilitaires EC2Config et EC2Launch offriront des fonctionnalités et des informations supplémentaires lors de l'exécution sur le système Nitro, y compris sur les instances EC2 Bare Metal. Par défaut, le service EC2Config est inclus dans les AMI antérieures à Windows Server 2016. EC2Launch remplace EC2Config sur les AMI Windows Server 2016 et versions ultérieures.

Lorsque les services EC2Config et EC2Launch sont mis à jour, les nouvelles AMI Windows d'AWS comprennent la dernière version du service. Toutefois, vous devez mettre à jour vos propres AMI et instances Windows avec la version la plus récente d'EC2Config et d'EC2Launch.

Pour installer ou mettre à jour EC2Config

1. Téléchargez et décompressez le [programme d'installation d'EC2Config](#).
2. Exécutez `EC2Install.exe`. Pour obtenir une liste complète des options, exécutez `EC2Install` avec l'option `/?`. Par défaut, la configuration affiche les invites. Pour exécuter la commande sans invites, utilisez l'option `/quiet`.

Pour plus d'informations, consultez [Installer la dernière version d'EC2Config](#).

Pour installer ou mettre à jour EC2Launch

1. Si vous avez déjà installé et configuré EC2Launch sur une instance, effectuez une sauvegarde du fichier de configuration EC2Launch. Le processus d'installation ne conserve pas les modifications de ce fichier. Par défaut, le fichier se trouve dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Téléchargez [EC2-Windows-Launch.zip](#) dans un répertoire sur l'instance.

3. Téléchargez [install.ps1](#) dans le répertoire dans lequel vous avez téléchargé EC2-Windows-Launch.zip.
4. Exécutez `install.ps1`.

 Note

Afin d'éviter les erreurs d'installation, exécutez le script `install.ps1` en tant qu'administrateur.

5. Si vous avez effectué une sauvegarde du fichier de configuration EC2Launch, copiez-la dans le répertoire `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Pour plus d'informations, consultez [Configurer une instance Windows à l'aide d'EC2Launch](#).

Étape 5 : Installer le pilote du port série pour les instances nues

Le type d'instance `i3.metal` utilise un périphérique série basé sur PCI plutôt qu'un périphérique série basé sur le port d'I/O. Les AMI Windows les plus récentes utilisent automatiquement le périphérique série basé sur PCI et le pilote du port série est installé. Si vous n'utilisez pas une instance lancée à partir d'une AMI Windows fournie par Amazon ayant pour date 11/4/2018 ou une date ultérieure, vous devez installer le pilote du port série pour activer le périphérique série pour les fonctions EC2 telles que la génération de mot de passe et la sortie de la console. La dernière version des utilitaires EC2Config et EC2Launch prend également en charge `i3.metal` et offre des fonctionnalités supplémentaires. Suivez les instructions de l'étape 4 si vous ne l'avez pas déjà fait.

Pour installer le pilote du port série

1. [Téléchargez](#) le package de pilotes série le plus récent sur l'instance.
2. Extrayez le contenu du dossier, ouvrez le menu contextuel (clic droit) pour `aws_ser.INF` et choisissez `install` (installer).
3. Choisissez OK.

Étape 6 : Mettre à jour les paramètres de gestion de l'alimentation

La mise à jour suivante des paramètres de gestion de l'alimentation fait en sorte que les écrans ne s'éteignent jamais, ce qui permet d'arrêter normalement le système d'exploitation sur le système

Nitro. Toutes les AMI Windows fournies par Amazon à partir du 28 novembre 2018 présentent cette configuration par défaut.

1. Ouvrez une invite de commande ou une PowerShell session.
2. Exécutez les commandes suivantes :

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-  
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0  
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-  
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0  
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-  
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Étape 7 : Mettre à jour les pilotes de puce Intel pour des nouveaux types d'instance

Les types d'instance `u-6tb1.metal`, `u-9tb1.metal` et `u-12tb1.metal` utilisent du matériel nécessitant des pilotes de puce qui n'étaient pas installés auparavant sur les AMI Windows. Si vous n'utilisez pas une instance lancée à partir d'une AMI Windows fournie par Amazon datée du 19/11/2018 ou d'une date ultérieure, vous devez installer les pilotes à l'aide de l'utilitaire Intel Chipset INF.

Pour installer les pilotes de puce

1. [Téléchargez l'utilitaire de puce](#) sur l'instance.
2. Extrayez les fichiers.
3. Exécutez `SetupChipset.exe`.
4. Acceptez le contrat de licence logicielle Intel et installez les pilotes de puce.
5. Redémarrez l'instance.

(Alternative) Mettez à niveau les pilotes AWS PV, ENA et NVMe à l'aide de AWS Systems Manager

Le document d'automatisation `AWSSupport-UpgradeWindowsAWSDrivers` automatise les étapes décrites dans la première, la deuxième et la troisième étape. Cette méthode peut également réparer une instance pour laquelle les mises à niveau du pilote ont échoué.

Le document `AWSSupport-UpgradeWindowsAWSDrivers` d'automatisation met à niveau ou répare le stockage et AWS les pilotes réseau sur l'instance EC2 spécifiée. Le document tente d'installer les dernières versions des AWS pilotes en ligne en appelant l' AWS Systems Manager agent (agent SSM). Si l'agent SSM n'est pas joignable, le document peut effectuer une installation hors ligne des AWS pilotes si cela est explicitement demandé.

 Note

Cette procédure échouera sur un contrôleur de domaine. Pour mettre à jour les pilotes sur un contrôleur de domaine, consultez [Mettre à niveau un contrôleur de domaine \(mise à niveau AWS PV\)](#).

Pour mettre à niveau automatiquement les pilotes AWS PV, ENA et NVMe à l'aide de AWS Systems Manager

1. Ouvrez la console Systems Manager à l'adresse <https://console.aws.amazon.com/systems-manager>.
2. Choisissez Automatisation, puis Exécute automation (Exécuter l'automatisation).
3. Recherchez puis sélectionnez le document `AWSSupport- UpgradeWindows AWSDrivers` automatisation, puis choisissez Exécuter l'automatisation.
4. Dans la section Paramètres d'entrée, configurez les options suivantes :

ID d'instance

Saisissez l'ID unique de l'instance à mettre à niveau.

AllowOffline

(Facultatif) Choisissez l'une des options suivantes :

- `True` : choisissez cette option pour effectuer une installation hors ligne. L'instance est arrêtée et redémarrée pendant le processus de mise à niveau.

 Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instances sont effacées. Pour préserver les données qui se trouvent sur

les volumes de stockage d'instances, assurez-vous de les sauvegarder dans un stockage permanent.

- `False` : (par défaut) pour effectuer une installation en ligne, laissez cette option sélectionnée. L'instance est redémarrée pendant le processus de mise à niveau.

Important

Les mises à niveau en ligne et hors ligne créent une AMI avant de tenter les opérations de mise à niveau. L'AMI persiste une fois l'automatisation terminée. Sécurisez votre accès à l'AMI ou supprimez-la si elle n'est plus nécessaire.

SubnetId

(Facultatif) Entrez l'une des valeurs suivantes :

- `SelectedInstanceSubnet` : (par défaut) le processus de mise à niveau lance l'instance d'assistant dans le même sous-réseau que l'instance à mettre à niveau. Le sous-réseau doit autoriser la communication avec les points de terminaison Systems Manager (`ssm.*`).
- `CreateNewVPC` : le processus de mise à niveau lance l'instance d'assistant dans un nouveau VPC. Utilisez cette option si vous ne savez pas si le sous-réseau de l'instance cible autorise la communication avec les points de terminaison `ssm.*`. Votre utilisateur doit disposer de l'autorisation de créer un VPC.
- Un ID de sous-réseau spécifique : spécifiez l'ID d'un sous-réseau spécifique dans lequel lancer l'instance d'assistant. Le sous-réseau doit appartenir à la même zone de disponibilité que l'instance à mettre à niveau, et il doit autoriser la communication avec les points de terminaison `ssm.*`.

5. Sélectionnez `Execute` (Exécuter).

6. Laissez la mise à niveau s'effectuer. Une mise à niveau en ligne peut prendre 10 minutes, et une mise à niveau en ligne jusqu'à 25 minutes.

Migrer une instance Windows d'un type d'instance Nitro vers un type d'instance Xen

La procédure suivante suppose que vous exécutez actuellement un type d'instance basé sur Nitro et que vous migrez vers une instance basée sur le système Xen, telle que M4 ou C4. Pour connaître les spécifications relatives aux types d'instances, consultez le [guide des types d'instances Amazon](#)

[EC2](#). Effectuez les étapes suivantes avant la migration pour éviter les erreurs pendant le processus de démarrage.

Pour migrer de Nitro vers Xen

1. Sauvegardez vos données.
2. Vérifiez que votre [politique de SAN Windows autorise la](#) mise en ligne de volumes de stockage non root.
3. AWS Les pilotes PV doivent être installés et mis à niveau sur une instance Nitro avant de migrer vers une instance Xen. Pour connaître les étapes d'installation et de mise à niveau des pilotes AWS PV, voir [Partie 1 : Installation et mise à niveau des pilotes AWS PV](#).
4. Pour effectuer la mise à jour vers la dernière version, consultez EC2Launch v2. Consultez la section [Migrer vers EC2Launch v2](#) pour connaître les étapes.
5. Ouvrez une PowerShell session et exécutez la commande suivante en tant qu'administrateur pour sysprep les pilotes de périphériques. L'exécution de sysprep garantit que les pilotes de stockage de démarrage anticipé requis pour le démarrage sur des instances Xen sont correctement enregistrés auprès de Windows.

 Note

L'exécution de la commande à l'aide de versions PowerShell (x86) provoquera une erreur. Cette commande ajoute uniquement les pilotes de périphérique critiques de démarrage à la base de données des périphériques critiques. Elle n'exécute pas la préparation Sysprep complète.

```
Start-Process rundll32.exe sppnp.dll, Sysprep_Generalize_Pnp -wait
```

6. Effectuez la migration vers un type d'instance Xen une fois le processus sysprep terminé.

Assistant de replateforme Windows vers Linux pour les bases de données Microsoft SQL Server

Pour plus d'informations sur la replateforme de bases de données Microsoft SQL Server de Windows vers Linux, consultez l'[assistant de replateforme Windows vers Linux pour les bases de données Microsoft SQL Server dans](#) le guide de l'utilisateur de Microsoft SQL Server sur Amazon EC2.

Résoudre les problèmes liés à une mise à niveau sur une instance

Windows

AWS fournit un support de mise à niveau pour les problèmes liés au service Upgrade Helper, un AWS utilitaire qui vous aide à effectuer des mises à niveau sur place impliquant des pilotes PV Citrix.

Après la mise à niveau, l'instance peut présenter temporairement une utilisation de l'unité centrale supérieure à la moyenne lorsque le service .NET Runtime Optimization optimise .NET framework. Ce comportement est normal.

Si l'instance n'a pas validé les deux contrôles des statuts au bout de plusieurs heures, effectuez les vérifications suivantes.

- Si vous avez mis à niveau vers Windows Server 2008 et que les deux contrôles de statut échouent au bout de plusieurs heures, la mise à niveau peut avoir échoué et présenter l'invite Cliquez sur OK pour confirmer la restauration. Du fait que la console n'est pas accessible dans cet état, il n'est pas possible de cliquer sur le bouton. Pour résoudre ce problème, effectuez un redémarrage via la console Amazon EC2 ou l'API. Le redémarrage prend au moins dix minutes pour s'initier. L'instance peut devenir disponible au bout de 25 minutes.
- Supprimez les applications ou les rôles de serveur du serveur et réessayez.

Si l'instance ne valide pas les deux contrôles de statut après la suppression des applications ou des rôles de serveur du serveur, procédez comme suit.

- Arrêtez l'instance et attachez le volume racine à une autre instance. Pour plus d'informations, consultez la description de la méthode pour arrêter et attacher le volume racine à une autre instance dans [« En attente du service de métadonnées »](#).
- Analysez les [fichiers journaux et d'événements de l'installation Windows](#) pour rechercher les échecs.

Pour tous les autres problèmes liés à la mise à niveau ou à la migration d'un système d'exploitation, nous vous recommandons de consulter les articles répertoriés dans [Avant de commencer une mise à niveau sur place](#).

Flotte EC2 et parc d'instances Spot

Les flottes EC2 et les parcs d'instances Spot sont conçus pour être un moyen utile de lancer une flotte (ou un groupe) d'instances avec AWS. Chaque instance d'un parc est basée sur un [modèle de lancement](#) ou un ensemble de paramètres de lancement que vous configurez manuellement lors du lancement.

Les flottes offrent les caractéristiques et avantages suivants. Ces avantages vous permettent de maximiser les économies et d'optimiser la disponibilité et les performances lorsque vous exécutez des applications sur plusieurs instances EC2.

Types d'instances et options d'achat multiples

En un seul appel d'API, une flotte peut lancer plusieurs types d'instances et options d'achat (Instances Spot et à la demande), ce qui vous permet d'optimiser les coûts grâce à l'utilisation d'Instances Spot. Vous pouvez également profiter des remises sur les instances réservées et les Savings Plan en les utilisant conjointement avec les instances à la demande au sein de la flotte.

Répartition des instances dans les zones de disponibilité

Une flotte d'instances tente automatiquement de répartir uniformément les instances sur plusieurs zones de disponibilité pour une haute disponibilité. Cela garantit la résilience en cas d'indisponibilité d'une zone de disponibilité.

Remplacement automatique des instances Spot

Si votre flotte comprend des instances Spot, elle peut automatiquement demander une capacité Spot de remplacement si vos instances Spot sont interrompues ou sont altérées en raison d'une modification de l'état de l'instance. Grâce au rééquilibrage des capacités, une flotte d'instances Spot peut également surveiller et remplacer de manière proactive vos instances Spot qui présentent un risque d'interruption élevé.

EC2 Fleet est une bonne option si vous avez besoin de flexibilité pour gérer certains aspects du cycle de vie de l'instance ou les mécanismes de dimensionnement. Vous pouvez également utiliser les parcs d'instances Spot, mais nous ne vous le recommandons pas, car il s'agit d'une ancienne API pour laquelle aucun investissement n'est prévu. Toutefois, si vous utilisez déjà un parc d'instances Spot, vous pouvez continuer à l'utiliser. Les flottes EC2 et les parcs d'instances Spot offrent les mêmes fonctionnalités de base.

i Tip

En règle générale, nous vous recommandons de lancer des flottes d'instances ponctuelles et à la demande avec Amazon EC2 Auto Scaling, car cela fournit des fonctionnalités supplémentaires que vous pouvez utiliser pour gérer votre flotte. La liste des fonctionnalités supplémentaires inclut le remplacement automatique des surveillances de l'état pour les instances Spot et à la demande, les surveillances de l'état basées sur les applications et une intégration avec Elastic Load Balancing pour garantir une répartition uniforme du trafic applicatif vers vos instances saines. Vous pouvez également utiliser les groupes Auto Scaling lorsque vous utilisez AWS des services tels qu'Amazon ECS, Amazon EKS (groupes de nœuds autogérés) et Amazon VPC Lattice. Pour plus d'informations, consultez le [Guide de l'utilisateur Amazon EC2 Auto Scaling](#).

Rubriques

- [EC2 Fleet](#)
- [Parc d'instances Spot](#)
- [Surveillez les événements de votre flotte à l'aide d'Amazon EventBridge](#)
- [Tutoriels pour les flottes d'instances EC2 et Spot](#)
- [Exemples de configurations pour les flottes d'instances EC2 et Spot](#)
- [Quotas liés aux flottes](#)

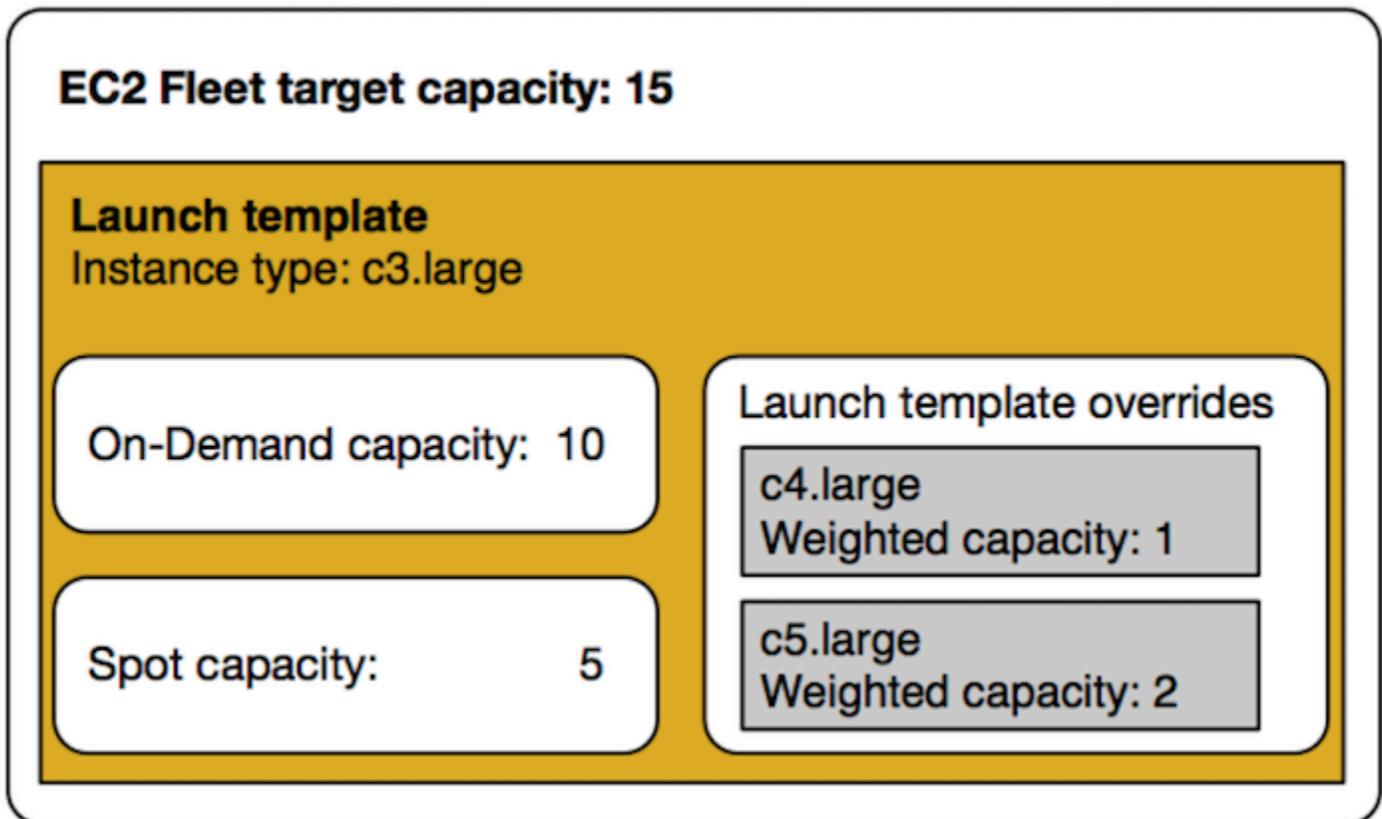
EC2 Fleet

Une flotte EC2 contient les informations de configuration permettant de lancer une flotte (ou un groupe) d'instances. En un seul appel d'API, une flotte peut lancer plusieurs types d'instances dans plusieurs zones de disponibilité, en utilisant conjointement les options d'achat d'instance Spot, d'instance à la demande, d'instance réservée et de Savings Plans. La flotte EC2 vous permet d'effectuer les opérations suivantes :

- Définir des cibles de capacité Spot et à la demande distinctes et le montant maximum que vous êtes prêt à payer par heure.
- Spécifier les types d'instance qui fonctionnent le mieux pour vos applications.
- Spécifiez comment Amazon EC2 doit répartir votre capacité de flotte au sein de chaque option d'achat

Vous pouvez également définir le montant maximum que vous êtes prêt à payer par heure pour votre flotte et une flotte EC2 lance les instances jusqu'à ce que le montant maximum soit atteint. Une fois le montant maximum que vous êtes prêt à payer atteint, la flotte arrête de lancer des instances même si la capacité cible n'a pas été atteinte.

La flotte EC2 tente de lancer le nombre d'instances nécessaires conformément à la capacité cible que vous avez spécifiée dans votre demande. Si vous avez spécifié un prix maximum total par heure, il remplit la capacité jusqu'à ce que le montant maximum que vous êtes prêt à payer soit atteint. Le flotte tente également de préserver la flotte de capacité cible si instances Spot est interrompu. Pour plus d'informations, veuillez consulter [Fonctionnement des instances Spot](#).



Vous pouvez spécifier un nombre illimité de types d'instance par flotte EC2. Ces types d'instance peuvent être alloués à l'aide des options d'achat à la demande et Spot. Vous pouvez aussi sélectionner plusieurs zones de disponibilité, spécifier différents prix Spot maximum pour chaque instance et choisir des options Spot supplémentaires pour flotte. Amazon EC2 utilise les options spécifiées pour allouer la capacité lors du lancement de la flotte.

Lorsque la flotte est en cours d'exécution, si Amazon EC2 récupère une instance Spot en raison d'une augmentation de prix ou de la défaillance d'une instance, la flotte EC2 peut essayer de remplacer les instances par l'un des types d'instance que vous spécifiez. Il est ainsi plus facile de

recupérer de la capacité de lors d'un pic de tarification Spot. Vous pouvez développer une stratégie de ressources flexible et élastique pour chaque flotte d'instances. Par exemple, au sein de flottes spécifiques, votre capacité principale peut être à la demande, complétée par une capacité spot moins onéreuse si possible.

Si vous avez des instances réservées et que vous spécifiez des instances à la demande dans votre flotte d'instances, la flotte EC2 utilise vos instances réservées. Par exemple, si votre flotte spécifie une instance à la demande en tant que `c4.large`, et que vous avez des instances réservées pour `c4.large`, vous recevez la tarification pour l'Instance réservée. Il en va de même si vous utilisez un Savings Plan.

L'utilisation d'une flotte EC2 n'entraîne pas de frais supplémentaires. Vous payez uniquement les instances EC2 que la flotte lance pour vous.

Sommaire

- [Limites flotte EC2](#)
- [instances à capacité extensible](#)
- [Types de demande flotte EC2](#)
- [Stratégies de configuration d'une flotte EC2](#)
- [Travailler avec Flottes EC2](#)

Limites flotte EC2

Les limites suivantes s'appliquent à une flotte EC2 :

- Une flotte EC2 est disponible uniquement via l'[API Amazon EC2](#), la [AWS CLI](#), les [kits SDK AWS](#), et la [AWS CloudFormation](#).
- Une demande de flotte EC2 ne peut pas couvrir plusieurs AWS régions. Vous devez créer une flotte EC2 distinct pour chaque région.
- Une demande de flotte EC2 ne peut pas couvrir différents sous-réseaux d'une même zone de disponibilité.

instances à capacité extensible

Si vous lancez vos instances Spot à l'aide d'un [type d'instance de performance à capacité extensible](#), et si vous prévoyez d'utiliser vos instances Spot de performance à capacité extensible

immédiatement et pour une courte durée, sans temps d'inactivité pour accumuler des crédits UC, nous vous recommandons de les lancer en [mode standard](#) pour éviter de payer des coûts plus élevés. Si vous lancez vos instances Spot de performance à capacité extensible en [mode Illimité](#) et que vous étendez immédiatement l'utilisation de l'UC, vous dépensez des crédits excédentaires pour cette extension d'utilisation. Si vous utilisez l'instance pour une courte durée, elle n'a pas le temps d'accumuler des crédits UC pour rembourser les crédits excédentaires, et ces derniers vous sont facturés lorsque vous résiliez l'instance.

Le mode Illimité convient aux instances Spot de performance à capacité extensible uniquement si l'instance s'exécute suffisamment longtemps pour accumuler des crédits UC pour l'extension d'utilisation. Sinon, payer des crédits excédentaires rend les instances Spot de performance à capacité extensible plus coûteuses que les autres instances. Pour plus d'informations, consultez [Quand utiliser le mode illimité/mode d'UC fixe ?](#).

Les crédits de lancement visent à optimiser la productivité du lancement initial des instances T2 en leur fournissant suffisamment de ressources de calcul pour pouvoir configurer l'instance. Il est interdit de procéder à des lancements répétés d'instances T2 pour bénéficier de nouveaux crédits de lancement. Si vous avez besoin de performances soutenues de l'UC, vous pouvez obtenir des crédits (en restant inactif pendant un certain temps) : utilisez le [mode Illimité](#) pour les instances Spot T2 ou un type d'instance avec UC dédiée.

Types de demande flotte EC2

Il existe trois types de demandes flotte EC2 :

`instant`

Si vous configurez le type de demande comme `instant`, Flotte EC2 passe une demande unique synchrone de la capacité souhaitée. Dans la réponse de l'API, il renvoie les instances qui ont été lancées, ainsi que les erreurs liées aux instances qui n'ont pas pu être lancées. Pour plus d'informations, consultez [Utilisez une flotte EC2 de type 'instantané'](#).

`request`

Si vous configurez le type de demande comme `request`, Flotte EC2 passe une demande unique asynchrone de la capacité souhaitée. Ensuite, si la capacité est réduite en raison d'interruptions Spot, la flotte d'instances n'essaie pas de réapprovisionner les instances Spot et il ne soumet pas les demandes dans d'autres groupes de capacité Spot si la capacité n'est pas disponible.

maintain

(Par défaut) Si vous configurez le type de demande comme `maintain`, Flotte EC2 passe une demande asynchrone de la capacité souhaitée et maintient la capacité en réapprovisionnant automatiquement les Instances Spot interrompues.

Les trois types de demandes bénéficient d'une stratégie d'allocation. Pour plus d'informations, consultez [Stratégies d'allocation pour instances Spot](#).

Utilisez une flotte EC2 de type 'instantané'

La flotte EC2 de type instantané est une demande synchrone unique qui ne réalise qu'une seule tentative de lancement de la capacité souhaitée. La réponse de l'API liste les instances qui ont été lancées, ainsi que les erreurs liées aux instances qui n'ont pas pu être lancées. Il y a plusieurs bénéfices à utiliser une flotte EC2 de type instantané, qui sont décrits dans cet article. Des exemples de configurations sont fournis à la fin de l'article.

Pour les charges de travail qui nécessitent une API de lancement uniquement pour lancer des instances EC2, vous pouvez utiliser l'API `RunInstances`. Toutefois, avec `RunInstances`, vous ne pouvez lancer que des instances à la demande ou des instances ponctuelles, mais pas les deux dans la même demande. En outre, lorsque vous lancez `RunInstances` des instances Spot, votre demande d'instance Spot est limitée à un type d'instance et à une zone de disponibilité. Ceci cible un seul groupe de capacité Spot (ensemble d'instances inutilisées ayant le même type d'instance et la même zone de disponibilité). Si le pool de capacité Spot ne dispose pas d'une capacité d'instance Spot suffisante pour votre demande, l'appel `RunInstances` échoue.

Au lieu de l'utiliser `RunInstances` pour lancer des instances Spot, nous vous recommandons d'utiliser l'API `CreateFleet` avec le type paramètre défini sur `instant` pour bénéficier des avantages suivants :

- Launch On-Demand instances and Spot instances in one request. (Lancez des instances à la demande et des instances Spot en une seule demande.) Une flotte EC2 peut lancer des instances à la demande et/ou des instances Spot. La demande des instances Spot est satisfaite si la capacité disponible et le prix maximum par heure que vous avez spécifié pour la demande dépassent le prix spot actuel.
- Increase the availability of Spot instances. (Augmentez la disponibilité des instances Spot.). En utilisant une flotte EC2 de type `instant`, vous pouvez lancer des instances Spot en suivant les

[Spot best practices](#) (Bonnes pratiques en matière d'instances Spot) avec les avantages qui en résultent :

- Bonnes pratiques en matière d'instances Spot : Soyez flexible en ce qui concerne les types d'instance et les zones de disponibilité.

Bénéfices : en spécifiant plusieurs types d'instance et zones de disponibilité, vous augmentez le nombre de groupes de capacités Spot. Cela donne au service Spot une meilleure chance de trouver et d'allouer la capacité de calcul Spot souhaitée. Une bonne pratique consiste à être flexible et à choisir au moins 10 types d'instances pour chaque charge de travail et à s'assurer que toutes les zones de disponibilité sont configurées pour être utilisées dans votre VPC.

- Repérez les meilleures pratiques : utilisez la stratégie price-capacity-optimized d'allocation.

Avantage : la stratégie price-capacity-optimized d'allocation identifie les instances parmi les pools de capacité ponctuels les plus disponibles, puis provisionne automatiquement les instances à partir des pools les moins chers de ces pools. Étant donné que votre capacité d'instance Spot provient de groupes avec une capacité optimale, cela réduit la possibilité que vos instances Spot soient arrêtées pour être récupérées par Amazon EC2.

- Get access to a wider set of capabilities. (Accédez à un ensemble plus large de fonctionnalités). Pour les charges de travail qui nécessitent une API de lancement uniquement et pour lesquelles vous préférez gérer le cycle de vie de votre instance plutôt que de laisser EC2 Fleet le gérer à votre place, utilisez le type instant de flotte EC2 plutôt que l'API. [RunInstances](#) EC2 Fleet fournit un ensemble de fonctionnalités plus RunInstances large que ce que montrent les exemples suivants. Pour toutes les autres charges de travail, vous devez utiliser Amazon EC2 Auto Scaling, car il fournit un ensemble de ressources plus complet pour une plus grande variété de charges de travail, telles que les charges de travail basées sur ELB, les charges de travail conteneurisées et les tâches de traitement de file d'attente.

Vous pouvez utiliser la flotte d'EC2 de type instantané pour lancer des instances dans des blocs de capacité. Pour plus d'informations, consultez [Tutoriel : Lancer des instances dans des blocs de capacité](#).

AWS des services tels qu'Amazon EC2 Auto Scaling et Amazon EMR utilisent EC2 Fleet de type instantané pour lancer des instances EC2.

Conditions préalables pour les flottes EC2 de type instantané

Pour connaître les conditions préalables à la création d'une flotte EC2, veuillez consulter [Conditions préalables requises flotte EC2](#).

Comment fonctionne une flotte EC2 instantanée

Lorsque vous travaillez avec une flotte EC2 de type instant, la séquence d'événements est la suivante :

1. Configurez le type de [CreateFleet](#) demande en tant que instant. Pour plus d'informations, consultez [Créer une flotte EC2](#). Notez qu'après avoir effectué l'appel d'API, vous ne pouvez plus le modifier.
2. Lorsque vous effectuez l'appel d'API, la flotte EC2 passe une demande unique synchrone de la capacité souhaitée.
3. La réponse de l'API liste les instances qui ont été lancées, ainsi que les erreurs liées aux instances qui n'ont pas pu être lancées.
4. Vous pouvez décrire votre flotte EC2, répertorier les instances associées à votre flotte EC2 et consulter l'historique de votre flotte EC2.
5. Après le lancement de vos instances, vous pouvez [supprimer la demande de flotte](#). Lorsque vous supprimez la demande de flotte, vous pouvez également choisir de résilier les instances associées ou de les laisser en cours d'exécution.
6. Vous pouvez résilier les instances à tout moment.

Exemples

Les exemples suivants montrent comment utiliser une flotte EC2 de type instant pour différents cas d'utilisation. Pour plus d'informations sur l'utilisation des paramètres de l' [CreateFleet](#) API EC2, consultez le [CreateFleet](#) manuel Amazon EC2 API Reference.

Exemples

- [Exemple 1 : Lancer des instances Spot avec la stratégie d'allocation optimisée pour la capacité](#)
- [Exemple 2 : Lancer une unique instance Spot avec la stratégie d'allocation optimisée pour la capacité](#)
- [Exemple 3 : Lancer des instances Spot en utilisant la pondération d'instance](#)
- [Exemple 4 : Lancer des instances Spot dans une seule zone de disponibilité](#)
- [Exemple 5 : Lancer des instances Spot de type d'instance unique dans une seule zone de disponibilité](#)
- [Exemple 6 : Lancer des instances Spot uniquement si une capacité cible minimale peut être lancée](#)

- [Exemple 7 : Lancer des instances Spot uniquement si une capacité cible minimale du même type d'instance et dans une seule zone de disponibilité peut être lancée](#)
- [Exemple 8 : Lancer des instances avec plusieurs modèles de lancement](#)
- [Exemple 9 : Lancer des instances Spot avec une base d'instances à la demande](#)
- [Exemple 10 : Lancer des instances Spot à l'aide d'une stratégie d'allocation optimisée pour la capacité avec une base d'instances à la demande en utilisant des réservations de capacité et la stratégie d'allocation prioritaire](#)
- [Exemple 11 : Lancer des instances ponctuelles à l'aide d' capacity-optimized-prioritized une stratégie d'allocation](#)

Exemple 1 : Lancer des instances Spot avec la stratégie d'allocation optimisée pour la capacité

L'exemple suivant spécifie les paramètres requis dans une flotte EC2 de type instant : un modèle de lancement, une capacité cible, une option d'achat par défaut et des remplacements du modèle de lancement.

- Le modèle de lancement est identifié par son nom de modèle de lancement et son numéro de version.
- Les 12 remplacements de modèle de lancement spécifient 4 types d'instance différents et 3 sous-réseaux différents, chacun dans une zone de disponibilité distincte. Chaque combinaison de type d'instance et de sous-réseau définit un groupe de capacités Spot, ce qui donne un total de 12 groupes de capacités Spot.
- La capacité cible pour la flotte est de 20 instances.
- L'option d'achat par défaut est spot, ce qui fait que la flotte tente de lancer 20 instances Spot dans le groupe de capacités Spot avec une capacité optimale pour le nombre d'instances qui sont lancées.

```
{
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized"
  },
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "ec2-fleet-1t1",
        "Version": "$Latest"
      }
    }
  ]
}
```

```
},
"Overrides":[
  {
    "InstanceType":"c5.large",
    "SubnetId":"subnet-fae8c380"
  },
  {
    "InstanceType":"c5.large",
    "SubnetId":"subnet-e7188bab"
  },
  {
    "InstanceType":"c5.large",
    "SubnetId":"subnet-49e41922"
  },
  {
    "InstanceType":"c5d.large",
    "SubnetId":"subnet-fae8c380"
  },
  {
    "InstanceType":"c5d.large",
    "SubnetId":"subnet-e7188bab"
  },
  {
    "InstanceType":"c5d.large",
    "SubnetId":"subnet-49e41922"
  },
  {
    "InstanceType":"m5.large",
    "SubnetId":"subnet-fae8c380"
  },
  {
    "InstanceType":"m5.large",
    "SubnetId":"subnet-e7188bab"
  },
  {
    "InstanceType":"m5.large",
    "SubnetId":"subnet-49e41922"
  },
  {
    "InstanceType":"m5d.large",
    "SubnetId":"subnet-fae8c380"
  },
  {
    "InstanceType":"m5d.large",
```

```

        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-49e41922"
    }
]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}

```

Exemple 2 : Lancer une unique instance Spot avec la stratégie d'allocation optimisée pour la capacité

Vous pouvez lancer de manière optimale une instance Spot à la fois en effectuant plusieurs appels d'API EC2 instant Fleet de type 1. TotalTargetCapacity

L'exemple suivant spécifie les paramètres requis dans une flotte EC2 de type instant : un modèle de lancement, une capacité cible, une option d'achat par défaut et des remplacements de modèle de lancement. Le modèle de lancement est identifié par son nom de modèle de lancement et son numéro de version. Les 12 remplacements de modèle de lancement ont 4 types d'instance différents et 3 sous-réseaux différents, chacun dans une zone de disponibilité distincte. La capacité cible de la flotte est de 1 instance, et l'option d'achat par défaut est Spot, ce qui fait que la flotte tente de lancer une instance Spot à partir de l'un des 12 groupes de capacités Spot en fonction de la stratégie d'allocation optimisée pour la capacité, pour lancer une instance Spot à partir du groupe de capacités le plus disponible.

```

{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "ec2-fleet-1t1",
                "Version": "$Latest"
            },
            "Overrides": [

```

```
{
  "InstanceType": "c5.large",
  "SubnetId": "subnet-fae8c380"
},
{
  "InstanceType": "c5.large",
  "SubnetId": "subnet-e7188bab"
},
{
  "InstanceType": "c5.large",
  "SubnetId": "subnet-49e41922"
},
{
  "InstanceType": "c5d.large",
  "SubnetId": "subnet-fae8c380"
},
{
  "InstanceType": "c5d.large",
  "SubnetId": "subnet-e7188bab"
},
{
  "InstanceType": "c5d.large",
  "SubnetId": "subnet-49e41922"
},
{
  "InstanceType": "m5.large",
  "SubnetId": "subnet-fae8c380"
},
{
  "InstanceType": "m5.large",
  "SubnetId": "subnet-e7188bab"
},
{
  "InstanceType": "m5.large",
  "SubnetId": "subnet-49e41922"
},
{
  "InstanceType": "m5d.large",
  "SubnetId": "subnet-fae8c380"
},
{
  "InstanceType": "m5d.large",
  "SubnetId": "subnet-e7188bab"
},
}
```

```
        {
            "InstanceType": "m5d.large",
            "SubnetId": "subnet-49e41922"
        }
    ]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 1,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemple 3 : Lancer des instances Spot en utilisant la pondération d'instance

Les exemples suivants utilisent la pondération d'instance, ce qui signifie que le prix est déterminé par heure d'unité, et non par heure d'instance. Chaque configuration du lancement répertorie un type d'instance différent et un poids différent en fonction du nombre d'unités de la charge de travail pouvant s'exécuter sur l'instance en supposant qu'une unité de la charge de travail nécessite 15 Go de mémoire et 4 vCPU. Par exemple, une instance m5.xlarge (4 vCPUs et 16 Go de mémoire) peut exécuter une unité et est pondérée 1, une instance m5.2xlarge (8 vCPUs et 32 Go de mémoire) peut exécuter 2 unités et est pondérée 2, et ainsi de suite. La capacité cible totale est définie sur 40 unités. L'option d'achat par défaut est Spot et la stratégie d'allocation est optimisée pour la capacité, ce qui se traduit par 40 m5.xlarge (40 divisé par 1), 20 m5.2xlarge (40 divisé par 2), 10 m5.4xlarge (40 divisé par 4), 5 m5.8xlarge (40 divisé par 8) ou un mélange de types d'instances avec des pondérations totalisant la capacité désirée, sur la base de la stratégie d'allocation optimisée pour les capacités.

Pour plus d'informations, consultez [Pondération d'instance flotte EC2](#).

```
{
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized"
  },
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "ec2-fleet-lt1",
        "Version": "$Latest"
      },
      "Overrides": [
```

```
{
  "InstanceType": "m5.xlarge",
  "SubnetId": "subnet-fae8c380",
  "WeightedCapacity": 1
},
{
  "InstanceType": "m5.xlarge",
  "SubnetId": "subnet-e7188bab",
  "WeightedCapacity": 1
},
{
  "InstanceType": "m5.xlarge",
  "SubnetId": "subnet-49e41922",
  "WeightedCapacity": 1
},
{
  "InstanceType": "m5.2xlarge",
  "SubnetId": "subnet-fae8c380",
  "WeightedCapacity": 2
},
{
  "InstanceType": "m5.2xlarge",
  "SubnetId": "subnet-e7188bab",
  "WeightedCapacity": 2
},
{
  "InstanceType": "m5.2xlarge",
  "SubnetId": "subnet-49e41922",
  "WeightedCapacity": 2
},
{
  "InstanceType": "m5.4xlarge",
  "SubnetId": "subnet-fae8c380",
  "WeightedCapacity": 4
},
{
  "InstanceType": "m5.4xlarge",
  "SubnetId": "subnet-e7188bab",
  "WeightedCapacity": 4
},
{
  "InstanceType": "m5.4xlarge",
  "SubnetId": "subnet-49e41922",
  "WeightedCapacity": 4
}
```

```
    },
    {
      "InstanceType": "m5.8xlarge",
      "SubnetId": "subnet-fae8c380",
      "WeightedCapacity": 8
    },
    {
      "InstanceType": "m5.8xlarge",
      "SubnetId": "subnet-e7188bab",
      "WeightedCapacity": 8
    },
    {
      "InstanceType": "m5.8xlarge",
      "SubnetId": "subnet-49e41922",
      "WeightedCapacity": 8
    }
  ]
}
],
"TargetCapacitySpecification": {
  "TotalTargetCapacity": 40,
  "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemple 4 : Lancer des instances Spot dans une seule zone de disponibilité

Vous pouvez configurer un parc pour lancer toutes les instances dans une seule zone de disponibilité en définissant les options `Spot SingleAvailabilityZone` sur `true`.

Les 12 remplacements de modèle de lancement ont des types d'instance et des sous-réseaux différents (chacun dans une zone de disponibilité distincte), mais la même capacité pondérée. La capacité cible totale est de 20 instances, l'option d'achat par défaut est Spot et la stratégie d'allocation Spot est optimisée pour la capacité. La flotte EC2 lance 20 instances Spot, le toutes dans une seule AZ, à partir du ou des groupes de capacités Spot avec une capacité optimale en utilisant les spécifications de lancement.

```
{
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized",
    "SingleAvailabilityZone": true
  },
}
```



```

        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-49e41922"
    }
]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}

```

Exemple 5 : Lancer des instances Spot de type d'instance unique dans une seule zone de disponibilité

Vous pouvez configurer un parc pour lancer toutes les instances du même type et dans une seule zone de disponibilité en définissant `SpotOptions SingleInstanceType` les valeurs `true` et `SingleAvailabilityZone true`.

Les 12 remplacements de modèle de lancement ont des types d'instance et des sous-réseaux différents (chacun dans une zone de disponibilité distincte), mais la même capacité pondérée. La capacité cible totale est de 20 instances, l'option d'achat par défaut est Spot et la stratégie d'allocation Spot est optimisée pour la capacité. La flotte EC2 lance 20 instances Spot du même type d'instance, le tout dans une seule AZ à partir du groupe d'instances Spot avec une capacité optimale en utilisant les spécifications de lancement.

```

{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [

```

```
{
  "LaunchTemplateSpecification":{
    "LaunchTemplateName":"ec2-fleet-lt1",
    "Version":"$Latest"
  },
  "Overrides":[
    {
      "InstanceType":"c5.4xlarge",
      "SubnetId":"subnet-fae8c380"
    },
    {
      "InstanceType":"c5.4xlarge",
      "SubnetId":"subnet-e7188bab"
    },
    {
      "InstanceType":"c5.4xlarge",
      "SubnetId":"subnet-49e41922"
    },
    {
      "InstanceType":"c5d.4xlarge",
      "SubnetId":"subnet-fae8c380"
    },
    {
      "InstanceType":"c5d.4xlarge",
      "SubnetId":"subnet-e7188bab"
    },
    {
      "InstanceType":"c5d.4xlarge",
      "SubnetId":"subnet-49e41922"
    },
    {
      "InstanceType":"m5.4xlarge",
      "SubnetId":"subnet-fae8c380"
    },
    {
      "InstanceType":"m5.4xlarge",
      "SubnetId":"subnet-e7188bab"
    },
    {
      "InstanceType":"m5.4xlarge",
      "SubnetId":"subnet-49e41922"
    },
    {
      "InstanceType":"m5d.4xlarge",
```

```

        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-49e41922"
    }
]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}

```

Exemple 6 : Lancer des instances Spot uniquement si une capacité cible minimale peut être lancée

Vous pouvez configurer une flotte pour lancer des instances uniquement si la capacité cible minimale peut être lancée en définissant les options `MinTargetCapacity Spot` sur la capacité cible minimale que vous souhaitez lancer ensemble.

Les 12 remplacements de modèle de lancement ont des types d'instance et des sous-réseaux différents (chacun dans une zone de disponibilité distincte), mais la même capacité pondérée. La capacité cible totale et la capacité cible minimum sont toutes deux de 20 instances, l'option d'achat par défaut est Spot et la stratégie d'allocation Spot est optimisée pour la capacité. La flotte EC2 lance 20 instances Spot à partir du groupe de capacités Spot avec une capacité optimale à l'aide des remplacements du modèle de lancement, uniquement si elle peut lancer les 20 instances en même temps.

```

{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {

```

```
    "LaunchTemplateName":"ec2-fleet-1t1",
    "Version":"$Latest"
  },
  "Overrides":[
    {
      "InstanceType":"c5.4xlarge",
      "SubnetId":"subnet-fae8c380"
    },
    {
      "InstanceType":"c5.4xlarge",
      "SubnetId":"subnet-e7188bab"
    },
    {
      "InstanceType":"c5.4xlarge",
      "SubnetId":"subnet-49e41922"
    },
    {
      "InstanceType":"c5d.4xlarge",
      "SubnetId":"subnet-fae8c380"
    },
    {
      "InstanceType":"c5d.4xlarge",
      "SubnetId":"subnet-e7188bab"
    },
    {
      "InstanceType":"c5d.4xlarge",
      "SubnetId":"subnet-49e41922"
    },
    {
      "InstanceType":"m5.4xlarge",
      "SubnetId":"subnet-fae8c380"
    },
    {
      "InstanceType":"m5.4xlarge",
      "SubnetId":"subnet-e7188bab"
    },
    {
      "InstanceType":"m5.4xlarge",
      "SubnetId":"subnet-49e41922"
    },
    {
      "InstanceType":"m5d.4xlarge",
      "SubnetId":"subnet-fae8c380"
    },
  ],
}
```

```
    {
      "InstanceType": "m5d.4xlarge",
      "SubnetId": "subnet-e7188bab"
    },
    {
      "InstanceType": "m5d.4xlarge",
      "SubnetId": "subnet-49e41922"
    }
  ]
}
],
"TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemple 7 : Lancer des instances Spot uniquement si une capacité cible minimale du même type d'instance et dans une seule zone de disponibilité peut être lancée

Vous pouvez configurer un parc pour lancer des instances uniquement si la capacité cible minimale peut être lancée avec un seul type d'instance dans une seule zone de disponibilité en définissant les options `MinTargetCapacity Spot` sur la capacité cible minimale que vous souhaitez lancer en même temps que `SingleInstanceType` les `SingleAvailabilityZone` options.

Les 12 spécifications de lancement, qui remplacent le modèle de lancement, ont des types et des sous-réseaux d'instances différents (chacun dans une AZ différentes), mais la même capacité pondérée. La capacité cible totale et la capacité cible minimale sont toutes deux fixées à 20 instances, l'option d'achat par défaut est au comptant, la stratégie d'allocation au comptant est optimisée en termes de capacité, `SingleInstanceType` c'est vrai et `SingleAvailabilityZone` vrai. La flotte EC2 lance 20 instances Spot du même type d'instance, le tout dans une seule AZ à partir du groupe d'instances Spot avec une capacité optimale en utilisant les spécifications de lancement, mais uniquement si 20 instances peuvent être lancées en même temps.

```
{
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized",
    "SingleInstanceType": true,
    "SingleAvailabilityZone": true,
    "MinTargetCapacity": 20
  },
}
```



```
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-49e41922"
    }
]
},
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemple 8 : Lancer des instances avec plusieurs modèles de lancement

Vous pouvez configurer une flotte pour lancer des instances avec des spécifications de lancement différentes pour différents types d'instance ou un groupe de types d'instance, en spécifiant plusieurs modèles de lancement. Dans cet exemple, nous voulons avoir différentes tailles de volume EBS pour différents types d'instance et nous les avons configurées dans les modèles de lancement `ec2-fleet-lt-4xl`, `ec2-fleet-lt-9xl` et `ec2-fleet-lt-18xl`.

Dans cet exemple, nous utilisons 3 modèles de lancement différents pour les 3 types d'instance en fonction de leur taille. Les remplacements de spécification de lancement sur tous les modèles de lancement utilisent des pondérations d'instance basées sur les vCPU du type d'instance. La capacité cible totale est de 144 unités, l'option d'achat par défaut est Spot et la stratégie d'allocation Spot est optimisée pour la capacité. La flotte EC2 peut soit lancer 9 `c5n.4xlarge` (144 divisé par 16) en utilisant le modèle de lancement `ec2-fleet-4xl` ou 4 `c5n.9xlarge` (144 divisé par 36) en utilisant le modèle de lancement `ec2-fleet-9xl`, ou 2 `c5n.18xlarge` (144 divisé par 72) en utilisant le modèle de lancement `ec2-fleet-18xl`, ou un mélange des types d'instances avec des pondérations totalisant la capacité souhaitée sur la base de la stratégie d'allocation optimisée pour la capacité.

```
{
    "SpotOptions": {
```

```
    "AllocationStrategy": "capacity-optimized"
  },
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "ec2-fleet-lt-18x1",
        "Version": "$Latest"
      },
      "Overrides": [
        {
          "InstanceType": "c5n.18xlarge",
          "SubnetId": "subnet-fae8c380",
          "WeightedCapacity": 72
        },
        {
          "InstanceType": "c5n.18xlarge",
          "SubnetId": "subnet-e7188bab",
          "WeightedCapacity": 72
        },
        {
          "InstanceType": "c5n.18xlarge",
          "SubnetId": "subnet-49e41922",
          "WeightedCapacity": 72
        }
      ]
    },
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "ec2-fleet-lt-9x1",
        "Version": "$Latest"
      },
      "Overrides": [
        {
          "InstanceType": "c5n.9xlarge",
          "SubnetId": "subnet-fae8c380",
          "WeightedCapacity": 36
        },
        {
          "InstanceType": "c5n.9xlarge",
          "SubnetId": "subnet-e7188bab",
          "WeightedCapacity": 36
        },
        {
          "InstanceType": "c5n.9xlarge",
```

```

        "SubnetId": "subnet-49e41922",
        "WeightedCapacity": 36
    }
]
},
{
    "LaunchTemplateSpecification": {
        "LaunchTemplateName": "ec2-fleet-lt-4x1",
        "Version": "$Latest"
    },
    "Overrides": [
        {
            "InstanceType": "c5n.4xlarge",
            "SubnetId": "subnet-fae8c380",
            "WeightedCapacity": 16
        },
        {
            "InstanceType": "c5n.4xlarge",
            "SubnetId": "subnet-e7188bab",
            "WeightedCapacity": 16
        },
        {
            "InstanceType": "c5n.4xlarge",
            "SubnetId": "subnet-49e41922",
            "WeightedCapacity": 16
        }
    ]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 144,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}

```

Exemple 9 : Lancer des instances Spot avec une base d'instances à la demande

L'exemple suivant spécifie la capacité cible totale de 20 instances pour la flotte et une capacité cible de 5 instances à la demande. L'option d'achat par défaut est Spot. La flotte d'instances lance 5 instances à la demande comme spécifié, mais a besoin de lancer 15 instances supplémentaires pour assurer la capacité cible totale. L'option d'achat correspondant à la différence est calculée sous la forme $\text{TotalTargetCapacity} - \text{OnDemandTargetCapacity} = \text{DefaultTargetCapacityType}$, ce qui

permet à la flotte de lancer 15 instances ponctuelles qui constituent l'un des 12 pools de capacités ponctuelles sur la base de la stratégie d'allocation optimisée pour les capacités.

```
{
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized"
  },
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "ec2-fleet-lt1",
        "Version": "$Latest"
      },
      "Overrides": [
        {
          "InstanceType": "c5.large",
          "SubnetId": "subnet-fae8c380"
        },
        {
          "InstanceType": "c5.large",
          "SubnetId": "subnet-e7188bab"
        },
        {
          "InstanceType": "c5.large",
          "SubnetId": "subnet-49e41922"
        },
        {
          "InstanceType": "c5d.large",
          "SubnetId": "subnet-fae8c380"
        },
        {
          "InstanceType": "c5d.large",
          "SubnetId": "subnet-e7188bab"
        },
        {
          "InstanceType": "c5d.large",
          "SubnetId": "subnet-49e41922"
        },
        {
          "InstanceType": "m5.large",
          "SubnetId": "subnet-fae8c380"
        },
        {
```

```
        "InstanceType": "m5.large",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-49e41922"
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-49e41922"
    }
]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "OnDemandTargetCapacity": 5,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemple 10 : Lancer des instances Spot à l'aide d'une stratégie d'allocation optimisée pour la capacité avec une base d'instances à la demande en utilisant des réservations de capacité et la stratégie d'allocation prioritaire

Vous pouvez configurer un parc pour qu'il utilise d'abord les réservations de capacité à la demande lorsque vous lancez une base d'instances à la demande avec le type de capacité cible par défaut comme emplacement en définissant la stratégie d'utilisation pour les réservations de capacité à `use-capacity-reservations-first`. Et si plusieurs groupes d'instances n'utilisent pas réservations de capacité, la stratégie d'allocation à la demande choisie est appliquée. Dans cet exemple, la stratégie d'allocation à la demande est prioritaire..

Dans cet exemple, il y a 6 réservations de capacité inutilisées disponibles. Cette capacité est inférieure à la capacité cible à la demande de la flotte de 10 instances à la demande.

Le compte dispose des 6 réservations de capacité suivantes inutilisées dans 2 groupes différents. Le nombre de réservations de capacité dans chaque pool est indiqué par AvailableInstanceCount.

```
{
  "CapacityReservationId": "cr-111",
  "InstanceType": "m5.large",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1a",
  "AvailableInstanceCount": 3,
  "InstanceMatchCriteria": "open",
  "State": "active"
}

{
  "CapacityReservationId": "cr-222",
  "InstanceType": "c5.large",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1a",
  "AvailableInstanceCount": 3,
  "InstanceMatchCriteria": "open",
  "State": "active"
}
```

La configuration de flotte suivante affiche uniquement les configurations pertinentes pour cet exemple. La stratégie d'allocation à la demande est priorisée, et la stratégie d'utilisation des réservations de capacité l'est use-capacity-reservations-first. La stratégie d'allocation Spot utilisée est optimisée au niveau de la capacité. La capacité cible totale est 20, la capacité cible à la demande est 10 et le type de capacité cible par défaut est spot.

```
{
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized"
  },
  "OnDemandOptions": {
    "CapacityReservationOptions": {
      "UsageStrategy": "use-capacity-reservations-first"
    },
    "AllocationStrategy": "prioritized"
  },
}
```

```
"LaunchTemplateConfigs": [  
  {  
    "LaunchTemplateSpecification":{  
      "LaunchTemplateName":"ec2-fleet-1t1",  
      "Version":"$Latest"  
    },  
    "Overrides":[  
      {  
        "InstanceType":"c5.large",  
        "SubnetId":"subnet-fae8c380",  
        "Priority": 1.0  
      },  
      {  
        "InstanceType":"c5.large",  
        "SubnetId":"subnet-e7188bab",  
        "Priority": 2.0  
      },  
      {  
        "InstanceType":"c5.large",  
        "SubnetId":"subnet-49e41922",  
        "Priority": 3.0  
      },  
      {  
        "InstanceType":"c5d.large",  
        "SubnetId":"subnet-fae8c380",  
        "Priority": 4.0  
      },  
      {  
        "InstanceType":"c5d.large",  
        "SubnetId":"subnet-e7188bab",  
        "Priority": 5.0  
      },  
      {  
        "InstanceType":"c5d.large",  
        "SubnetId":"subnet-49e41922",  
        "Priority": 6.0  
      },  
      {  
        "InstanceType":"m5.large",  
        "SubnetId":"subnet-fae8c380",  
        "Priority": 7.0  
      },  
      {  
        "InstanceType":"m5.large",
```

```

        "SubnetId": "subnet-e7188bab",
        "Priority": 8.0
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-49e41922",
        "Priority": 9.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-fae8c380",
        "Priority": 10.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-e7188bab",
        "Priority": 11.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-49e41922",
        "Priority": 12.0
    }
    ]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "OnDemandTargetCapacity": 10,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}

```

Après avoir créé la flotte instantanée à l'aide de la configuration précédente, les 20 instances suivantes sont lancées pour atteindre la capacité cible :

- 7 instances à la demande c5.large dans us-east-1a ; c5.large dans us-east-1a est priorisé en premier et il y a 3 réservations de capacité c5.large inutilisées disponibles. Les réservations de capacité sont d'abord utilisées pour lancer 3 instances à la demande, puis 4 instances à la demande supplémentaires sont lancées selon la stratégie d'allocation à la demande, qui est priorized dans cet exemple.

- 3 instances à la demande m5.large dans us-east-1a – m5.large dans us-east-1a est priorisé en second, et il y a 3 réservations de capacité c3.large inutilisées disponibles.
- 10 instances Spot issues de l'un des 12 groupes de capacités Spot ayant la capacité optimale selon la stratégie d'allocation optimisée pour cette capacité.

Une fois la flotte lancée, vous pouvez exécuter [describe-capacity-reservations](#) pour voir combien il reste de Réservations de capacité inutilisés. Dans cet exemple, vous devriez obtenir la réponse suivante, qui montre que toutes les réservations de capacité c5.large et m5.large ont été utilisées.

```
{
  "CapacityReservationId": "cr-111",
  "InstanceType": "m5.large",
  "AvailableInstanceCount": 0
}

{
  "CapacityReservationId": "cr-222",
  "InstanceType": "c5.large",
  "AvailableInstanceCount": 0
}
```

Exemple 11 : Lancer des instances ponctuelles à l'aide d' capacity-optimized-prioritized une stratégie d'allocation

L'exemple suivant spécifie les paramètres requis dans une flotte EC2 de type instant : un modèle de lancement, une capacité cible, une option d'achat par défaut et des remplacements de modèle de lancement. Le modèle de lancement est identifié par son nom de modèle de lancement et son numéro de version. Les 12 spécifications de lancement qui remplacent le modèle de lancement ont 4 types d'instance différents avec une priorité assignée, et 3 sous-réseaux différents, chacun dans une zone de disponibilité distincte. La capacité cible du parc est de 20 instances, et l'option d'achat par défaut est le spot, ce qui amène le parc à tenter de lancer 20 instances ponctuelles à partir de l'un des 12 pools de capacités ponctuelles sur la base de la stratégie d' capacity-optimized-prioritized allocation, qui met en œuvre les priorités au mieux, mais optimise d'abord la capacité.

```
{
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized-prioritized"
  },
  "LaunchTemplateConfigs": [
```

```
{
  "LaunchTemplateSpecification":{
    "LaunchTemplateName":"ec2-fleet-lt1",
    "Version":"$Latest"
  },
  "Overrides":[
    {
      "InstanceType":"c5.large",
      "SubnetId":"subnet-fae8c380",
      "Priority": 1.0
    },
    {
      "InstanceType":"c5.large",
      "SubnetId":"subnet-e7188bab",
      "Priority": 1.0
    },
    {
      "InstanceType":"c5.large",
      "SubnetId":"subnet-49e41922",
      "Priority": 1.0
    },
    {
      "InstanceType":"c5d.large",
      "SubnetId":"subnet-fae8c380",
      "Priority": 2.0
    },
    {
      "InstanceType":"c5d.large",
      "SubnetId":"subnet-e7188bab",
      "Priority": 2.0
    },
    {
      "InstanceType":"c5d.large",
      "SubnetId":"subnet-49e41922",
      "Priority": 2.0
    },
    {
      "InstanceType":"m5.large",
      "SubnetId":"subnet-fae8c380",
      "Priority": 3.0
    },
    {
      "InstanceType":"m5.large",
      "SubnetId":"subnet-e7188bab",
```

```
        "Priority": 3.0
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-49e41922",
        "Priority": 3.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-fae8c380",
        "Priority": 4.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-e7188bab",
        "Priority": 4.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-49e41922",
        "Priority": 4.0
    }
]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Stratégies de configuration d'une flotte EC2

Un Flotte EC2 est un groupe d'Instances à la demande et d'Instances Spot. La flotte d'EC2 peut également être un groupe d'instances de blocs de capacité.

Instances à la demande et instances Spot

La flotte EC2 tente de lancer le nombre d'instances nécessaires pour répondre à la capacité cible que vous spécifiez dans votre demande. Le flotte peut comprendre uniquement des instances à la demande uniquement des instances Spot, ou une combinaison d'instances à la demande et d'instances Spot. La demande des instances Spot est satisfaite si la capacité disponible et le prix

maximum par heure que vous avez spécifié pour la demande dépassent le prix spot actuel. Le flotte tente également de préserver la flotte de capacité cible si instances Spot est interrompu.

Vous pouvez également définir le montant maximum que vous être prêt à payer par heure pour votre flotte et flotte EC2 lance les instances jusqu'à ce que le montant maximum soit atteint. Une fois le montant maximum que vous être prêt à payer atteint, la flotte arrête de lancer des instances même si la capacité cible n'a pas été atteinte.

Un groupe de capacité Spot est un ensemble d'instances EC2 inutilisées avec le même type d'instance et la même zone de disponibilité. Lorsque vous créez une flotte EC2, vous pouvez inclure plusieurs spécifications de lancement qui varient en terme de type d'instance, zone de disponibilité, sous-réseau ou prix maximum. Le flotte d'instances sélectionne les groupes de capacité Spot servant à satisfaire la demande, selon les spécifications de lancement incluses dans votre demande et la configuration de cette demande. Les instances Spot proviennent des groupes sélectionnés.

Une flotte EC2 vous permet d'allouer un gros volume de capacité EC2 logique pour votre application sur la base du nombre de cœurs ou d'instances, ou de la quantité de mémoire. Par exemple, vous pouvez spécifier une flotte EC2 pour lancer une capacité cible de 200 instances, dont 130 sont des instances à la demande et le reste des instances Spot.

Instances de blocs de capacité

Les blocs de capacité pour ML vous permettent de réserver des instances GPU à une date ultérieure pour prendre en charge vos charges de travail de machine learning (ML) de courte durée. Les instances qui s'exécutent dans un bloc de capacité sont automatiquement placées à proximité les unes des autres dans [Amazon EC2 UltraClusters](#). Pour plus d'informations sur les blocs de capacité, consultez la section [Blocs de capacité pour ML](#) (français non garanti).

Utilisez les stratégies de configuration appropriées pour créer une flotte EC2 qui réponde à vos besoins.

Table des matières

- [Planification d'une flotte EC2](#)
- [Stratégies d'allocation pour instances Spot](#)
- [Sélection de type d'instance basée sur des attributs pour la flotte EC2](#)
- [Configurer flotte EC2 pour la sauvegarde à la demande](#)
- [Rééquilibrage de la capacité](#)
- [Remplacements du prix maximum](#)

- [Contrôle des dépenses](#)
- [Pondération d'instance flotte EC2](#)

Planification d'une flotte EC2

Lors de la planification de votre flotte EC2, nous vous recommandons de procéder comme suit :

- Déterminez si vous souhaitez créer une flotte EC2 qui envoie une demande unique synchrone ou asynchrone pour la capacité cible souhaitée ou qui conserve une capacité cible au fil du temps. Pour plus d'informations, veuillez consulter [Types de demande flotte EC2](#).
- Déterminez les types d'instance qui correspondent aux exigences de votre application.
- Si vous envisagez d'inclure des Instances Spot dans votre Flotte EC2, passez en revue les [bonnes pratiques en matière d'instances Spot](#) avant de créer le parc d'instances. Appuyez-vous sur ces bonnes pratiques lorsque vous planifiez votre flotte d'instances afin de pouvoir mettre en service ces instances au prix le plus bas possible.
- Déterminez la capacité cible de votre flotte EC2. Vous pouvez définir la capacité cible en instances ou en unités personnalisées. Pour plus d'informations, veuillez consulter [Pondération d'instance flotte EC2](#).
- Déterminez quelle portion de la capacité cible de la flotte EC2 doit correspondre à la capacité à la demande et à la capacité des instances spot. Vous pouvez spécifier 0 pour la capacité à la demande, pour la capacité des instances spot, ou pour les deux.
- Déterminez le prix par unité si vous avez recours à la pondération d'instance. Pour calculer le prix par unité, divisez le prix pour une heure d'instance par le nombre d'unités (ou pondération) que cette instance représente. Si vous n'utilisez pas la pondération d'instance, le prix par unité défini par défaut est le prix par heure d'instance.
- Déterminez le montant maximum par heure que vous êtes prêt à payer pour votre flotte. Pour plus d'informations, veuillez consulter [Contrôle des dépenses](#).
- Passez en revue les options possibles pour votre flotte EC2. Pour plus d'informations sur les paramètres de flotte, consultez [create-fleet](#) dans la Référence des commandes AWS CLI . Pour accéder à des exemples de configuration de Flotte EC2, consultez [Exemples de configuration d'une flotte EC2](#).

Stratégies d'allocation pour instances Spot

Votre configuration du lancement détermine tous les groupes de capacité Spot possibles (types d'instance et zones de disponibilité) à partir desquels la flotte EC2 peut lancer des instances Spot. Cependant, lors du lancement des instances, la flotte EC2 utilise la stratégie d'allocation que vous spécifiez pour choisir les groupes spécifiques parmi tous vos groupes possibles.

Note

(Instances Linux uniquement) Si vous configurez votre instance Spot pour qu'elle soit lancée alors qu'[AMD SEV-SNP](#) est activé, des frais d'utilisation horaires supplémentaires équivalant à 10 % du [taux horaire à la demande pour le type](#) d'instance sélectionné vous sont facturés. Si la stratégie d'allocation utilise le prix comme entrée, la flotte EC2 n'inclut pas ces frais supplémentaires ; seul le prix Spot est utilisé.

Stratégies d'allocation

Vous pouvez spécifier l'une des stratégies d'allocation suivantes pour les instances Spot :

`price-capacity-optimized`(recommandé)

La flotte EC2 identifie les groupes dotés des capacités disponibles les plus élevées pour le nombre d'instances qui sont lancées. Cela signifie que nous demanderons des instances Spot auprès des groupes qui, selon nous, présentent le moins de risques d'interruption à court terme. La flotte EC2 demande ensuite des instances Spot auprès du groupe le moins coûteux de ces groupes.

La stratégie d'allocation `price-capacity-optimized` constitue le meilleur choix pour la plupart des charges de travail Spot, telles que les applications conteneurisées sans état, les microservices, les applications Web, les tâches de données et d'analyse, ainsi que le traitement par lots.

`capacity-optimized`

La flotte EC2 identifie les groupes dotés des capacités disponibles les plus élevées pour le nombre d'instances qui sont lancées. Cela signifie que nous demanderons des instances Spot auprès des groupes qui, selon nous, présentent le moins de risques d'interruption à court terme. Vous pouvez éventuellement définir une priorité pour chaque type d'instance de votre parc à l'aide

de la commande `capacity-optimized-prioritized`. La flotte EC2 respecte les priorités de type d'instance sur la base du meilleur effort, mais optimise d'abord la capacité.

Avec les instances Spot, la tarification change lentement au fil du temps en fonction des tendances à long terme en matière d'offre et de demande, mais la capacité fluctue en temps réel. La stratégie `capacity-optimized` lance automatiquement des Instances Spot dans les pools les plus disponibles en examinant les données de capacité en temps réel et en prédisant les instances les plus disponibles. Cela convient parfaitement aux charges de travail dont l'interruption entraîne des coûts plus élevés associés au travail de redémarrage, telles que le temps d'intégration continue (CI), le rendu d'images et de médias, le deep learning, ainsi que les charges de travail de calcul haute performance (HPC), qui peuvent avoir un coût d'interruption plus élevé associées au travail de redémarrage. En offrant la possibilité de moins d'interruptions, la stratégie `capacity-optimized` peut réduire le coût global de votre charge de travail.

Alternativement, vous pouvez utiliser la stratégie d'allocation `capacity-optimized-prioritized` avec un paramètre de priorité pour définir l'ordre des types d'instance à utiliser de la priorité la plus élevée à la plus basse. Vous pouvez définir la même priorité pour différents types d'instance. La flotte EC2 optimisera d'abord la capacité, mais respectera les priorités de type d'instance sur la base du meilleur effort (par exemple, si le respect des priorités n'affecte pas de manière significative la capacité de la flotte EC2 à fournir une capacité optimale). C'est une bonne option pour les charges de travail pour lesquelles la possibilité de perturbation doit être minimisée, mais la priorité de certains types d'instances est également importante. Notez que lorsque vous définissez la priorité sur `capacity-optimized-prioritized`, la même priorité est également appliquée à vos instances à la demande si l'option à la demande `AllocationStrategy` est définie sur `prioritized`.

`diversified`

Les instances Spot sont réparties sur tous les groupes de capacité Spot.

`lowest-price`(non recommandé)

 Warning

Nous ne recommandons pas la stratégie `lowest-price` d'allocation car c'est elle qui présente le risque d'interruption le plus élevé pour vos instances Spot.

Les instances Spot proviennent du groupe dont le tarif est le plus bas et qui dispose d'une capacité disponible. Il s'agit de la stratégie par défaut. Nous vous recommandons toutefois

de remplacer la valeur par défaut en spécifiant la stratégie d'allocation `price-capacity-optimized`.

Si le groupe le moins coûteux ne dispose pas de capacité, les instances Spot proviennent du groupe le moins coûteux suivant qui a une capacité disponible.

Si un groupe n'a plus de capacité avant de répondre à votre demande, la flotte EC2 continue de répondre à votre demande en puisant dans le groupe suivant le moins coûteux. Pour garantir que la capacité souhaitée est atteinte, vous pouvez recevoir des instances Spot de plusieurs groupes.

Cette stratégie prenant uniquement en compte que le prix des instances et non la capacité disponible, elle peut entraîner des taux d'interruption élevés.

InstancePoolsToUseCount

Nombre de groupes d'instances Spot auxquels allouer votre capacité Spot cible. Valide uniquement lorsque la stratégie d'allocation est définie sur `lowest-price`. La flotte EC2 sélectionne les groupes d'instances Spot les moins chers et répartit équitablement votre capacité Spot cible entre le nombre de groupes d'instances Spot que vous spécifiez.

Notez qu'EC2 Fleet tente de puiser au mieux des instances Spot dans le nombre de groupes que vous spécifiez. Si un groupe n'a plus de capacité Spot avant de répondre à votre capacité cible, la flotte EC2 continue de répondre à votre demande en puisant dans le groupe suivant le moins coûteux. Pour garantir l'atteinte de votre capacité cible, il se peut que vous receviez des instances Spot provenant d'un nombre de groupes supérieur à celui que vous avez spécifié. De même, si la plupart des pools n'ont pas de capacité Spot, il se peut que vous receviez votre capacité cible complète à partir d'un nombre de groupes inférieur à celui que vous avez spécifié.

Choisir la stratégie d'allocation appropriée

Vous pouvez optimiser votre flotte en fonction de votre cas d'utilisation en choisissant la stratégie d'allocation de points appropriée. Pour la capacité cible d'instance à la demande, la flotte EC2 sélectionne toujours le type d'instance le moins cher en fonction du prix à la demande public, tout en continuant à suivre la stratégie d'allocation (`price-capacity-optimized`, `capacity-optimized`, `diversified` ou `lowest-price`) pour les instances Spot.

Trouver un équilibre entre le prix le plus bas et la capacité disponible

Pour trouver un équilibre entre les groupes de capacité Spot les moins chers et les groupes de capacité Spot présentant la disponibilité de capacité la plus élevée, nous vous recommandons d'utiliser la stratégie d'allocation `price-capacity-optimized`. Cette stratégie prend des

décisions concernant les groupes auprès desquels il convient de demander des instances Spot en fonction à la fois du prix des groupes et de la capacité disponible des instances Spot dans ces groupes. Cela signifie que nous demanderons des instances Spot auprès des groupes qui, selon nous, présentent le moins de risques d'interruption à court terme, tout en tenant compte du prix.

Si votre flotte exécute des charges de travail résilientes et sans état, notamment des applications conteneurisées, des microservices, des applications web, des tâches de données et d'analyse et des traitements par lots, utilisez la stratégie d'allocation `price-capacity-optimized` pour optimiser les économies de coûts et la capacité disponible.

Si votre flotte exécute des charges de travail dont l'interruption entraîne des coûts plus élevés associés au travail de redémarrage, vous devez implémenter des points de contrôle afin que les applications puissent redémarrer à partir de ce point, si elles sont interrompues. En utilisant des points de contrôle, vous adaptez la stratégie d'allocation `price-capacity-optimized` à ces charges de travail, car elle alloue la capacité à partir des groupes les moins chers qui offrent également un faible taux d'interruption des instances Spot.

Pour un exemple de configuration utilisant la stratégie d'allocation `price-capacity-optimized`, reportez-vous à la section [Exemple 10 : Lancer des instances ponctuelles dans une `price-capacity-optimized` flotte](#).

Lorsque les charges de travail ont un coût d'interruption élevé

Vous pouvez éventuellement utiliser la stratégie `capacity-optimized` si vous exécutez des charges de travail utilisant des types d'instances dont le prix est similaire, ou lorsque le coût des interruptions est si important que toute économie de coûts est insuffisante par rapport à une augmentation marginale du nombre d'interruptions. Cette stratégie alloue la capacité à partir des groupes de capacité Spot les plus disponibles qui offrent la possibilité de moins d'interruptions, ce qui peut réduire le coût global de votre charge de travail. Pour un exemple de configuration utilisant la stratégie d'allocation `capacity-optimized`, reportez-vous à la section [Exemple 8 : Lancer des instances ponctuelles dans un parc à capacité optimisée](#).

Lorsque le risque d'interruption doit être minimisé, mais que la préférence pour certains types d'instance est importante, vous pouvez exprimer vos priorités de groupe en utilisant la stratégie d'allocation `capacity-optimized-prioritized`, puis définir l'ordre des types d'instance à utiliser de la priorité la plus élevée à la plus basse. Pour accéder à un exemple de configuration, consultez [Exemple 9 : Lancer des instances ponctuelles dans un parc à capacité optimisée avec des priorités](#).

Notez que lorsque vous définissez les priorités sur `capacity-optimized-prioritized`, les mêmes priorités sont également appliquées à vos instances à la demande si l'option à la demande `AllocationStrategy` est définie sur `prioritized`.

Lorsque votre charge de travail est flexible dans le temps et que la capacité disponible n'est pas un facteur

Si votre flotte est de petite taille ou si elle s'exécute pendant un temps limité, vous pouvez utiliser `price-capacity-optimized` pour maximiser vos économies tout en tenant compte de la capacité disponible.

Lorsque votre flotte est importante ou s'exécute pendant une longue période

Si votre parc est important ou qu'il s'exécute pendant une longue durée, vous pouvez améliorer sa disponibilité en répartissant les Instances Spot entre plusieurs groupes en utilisant la stratégie `diversified`. Par exemple, si votre flotte EC2 spécifie 10 groupes et une capacité cible de 100 instances, la flotte lance 10 instances Spot dans chaque groupe. Si le prix Spot d'un pool dépasse le prix maximum de ce pool, seul 10 % de votre flotte est touché. Avec cette stratégie, votre flotte est également moins affecté par les augmentations du prix Spot dans un pool au fil du temps. Avec la stratégie `diversified`, la flotte EC2 ne lance pas d'instances Spot dans des groupes dont le prix spot est supérieur ou égal au [prix à la demande](#).

Maintenir la capacité cible

Une fois les Instances Spot résiliées en raison d'un changement de prix Spot ou de la modification de la capacité disponible d'un groupe de capacité Spot, un Flotte EC2 de type `maintain` lance des Instances Spot de remplacement. La stratégie d'allocation détermine les groupes à partir desquels les instances de remplacement sont lancées, comme suit :

- Si la stratégie d'allocation est `price-capacity-optimized`, la flotte lance les instances de remplacement dans les groupes présentant le plus de capacités d'instances Spot disponibles, tout en tenant compte du prix et en identifiant les groupes les moins chers avec une capacité disponible élevée.
- Si la stratégie d'allocation `capacity-optimized` est sélectionnée, la flotte lance les instances de remplacement dans les groupes avec le plus de capacités d'instances Spot disponibles.
- Si la stratégie d'allocation est `diversified`, le parc d'instances répartit les Instances Spot de remplacement entre les groupes restants.

Sélection de type d'instance basée sur des attributs pour la flotte EC2

Lorsque vous créez une flotte EC2, vous devez spécifier un ou plusieurs types d'instance pour configurer les instances à la demande et les instances Spot de la flotte. Au lieu de spécifier manuellement les types d'instance, vous pouvez spécifier les attributs qu'une instance doit posséder, et Amazon EC2 identifiera tous les types d'instance avec ces attributs. C'est ce qu'on appelle la sélection de type d'instance basée sur des attributs. Par exemple, vous pouvez spécifier le nombre minimal et maximal de vCPU requis pour vos instances, et EC2 Fleet lancera les instances à l'aide de tous les types d'instance disponibles répondant à ces exigences de vCPU.

La sélection de type d'instance basée sur des attributs est idéale pour les charges de travail et les cadres qui peuvent être flexibles quant aux types d'instances qu'ils utilisent, par exemple lors de l'exécution de conteneurs ou de flottes web, du traitement de big data et de la mise en œuvre d'outils de CI/CD (intégration et déploiement continu).

Avantages

La sélection de type d'instance basée sur des attributs présente les avantages suivants :

- Utilisez facilement les bons types d'instances : compte tenu du grand nombre de types d'instances disponibles, la recherche des types d'instances adaptés à votre charge de travail peut prendre beaucoup de temps. Lorsque vous spécifiez des attributs d'instance, les types d'instance auront automatiquement les attributs requis pour votre charge de travail.
- Configuration simplifiée — Pour spécifier manuellement plusieurs types d'instances pour un parc EC2, vous devez créer un modèle de lancement distinct pour chaque type d'instance. Toutefois, avec la sélection de type d'instance basée sur des attributs, pour fournir plusieurs types d'instance, il suffit de spécifier les attributs d'instance dans le modèle de lancement ou dans un remplacement de modèle de lancement.
- Utilisation automatique de nouveaux types d'instances : lorsque vous spécifiez des attributs d'instance plutôt que des types d'instances, votre parc peut utiliser des types d'instances de nouvelle génération au fur et à mesure de leur publication, afin de « pérenniser » la configuration du parc.
- Flexibilité du type d'instance — Lorsque vous spécifiez des attributs d'instance plutôt que des types d'instance, EC2 Fleet peut choisir parmi un large éventail de types d'instances pour lancer des instances Spot, conformément aux [meilleures pratiques Spot en matière de flexibilité des types d'instance](#).

Rubriques

- [Fonctionnement de la sélection de type d'instance basée sur des attributs](#)
- [Protection des prix](#)
- [Considérations](#)
- [Créer une flotte EC2 avec une sélection de type d'instance basée sur des attributs](#)
- [Exemples de configurations valides et non valides](#)
- [Aperçu des types d'instances avec des attributs spécifiés](#)

Fonctionnement de la sélection de type d'instance basée sur des attributs

Pour utiliser la sélection de type d'instance basée sur des attributs dans la configuration de votre flotte, vous remplacez la liste des types d'instance par une liste d'attributs d'instance dont vos instances ont besoin. La flotte EC2 lance des instances sur tous les types d'instance disponibles possédant les attributs d'instance spécifiés.

Rubriques

- [Types d'attributs d'instance](#)
- [Où configurer la sélection de type d'instance basée sur des attributs](#)
- [Comment la flotte EC2 utilise la sélection de type d'instance basée sur des attributs lors de l'approvisionnement d'une flotte](#)

Types d'attributs d'instance

Il existe plusieurs attributs d'instance que vous pouvez spécifier pour exprimer vos besoins en matière de calcul, tels que :

- Nombre de vCPU : nombre minimum et maximum de vCPU par instance.
- Mémoire : mémoire minimale et maximale GiBs par instance.
- Stockage local : s'il faut utiliser EBS ou des volumes de stockage d'instance pour le stockage local.
- Performances éclatantes : s'il faut utiliser la famille d'instances T, y compris les types T4g, T3a, T3 et T2.

Pour une description de chaque attribut et des valeurs par défaut, consultez le [InstanceRequirements](#) manuel Amazon EC2 API Reference.

Où configurer la sélection de type d'instance basée sur des attributs

Selon que vous utilisez la console ou le AWS CLI, vous pouvez spécifier les attributs d'instance pour la sélection du type d'instance basée sur les attributs comme suit :

Dans la console, vous pouvez spécifier les attributs d'instance dans le composant de configuration de flotte suivant :

- Dans un modèle de lancement, puis référez le modèle de lancement dans la demande de flotte

Dans le AWS CLI, vous pouvez spécifier les attributs d'instance dans l'un ou l'ensemble des composants de configuration de flotte suivants :

- Dans un modèle de lancement, puis référez le modèle de lancement dans la demande de flotte
- Dans un remplacement de modèle de lancement

Si vous souhaitez combiner des instances utilisant différentes AMI, vous pouvez spécifier des attributs d'instance dans plusieurs remplacements de modèles de lancement. Par exemple, différents types d'instance peuvent utiliser des processeurs x86 et Arm.

Comment la flotte EC2 utilise la sélection de type d'instance basée sur des attributs lors de l'approvisionnement d'une flotte

La flotte EC2 alloue une flotte de la manière suivante :

- La flotte EC2 identifie les types d'instance qui possèdent les attributs spécifiés.
- La flotte EC2 utilise la protection des prix pour déterminer les types d'instances à exclure.
- EC2 Fleet détermine les pools de capacités à partir desquels il envisagera de lancer les instances en fonction des AWS régions ou des zones de disponibilité présentant les types d'instances correspondants.
- La flotte EC2 applique la stratégie d'allocation spécifiée pour déterminer les groupes de capacités à partir desquels lancer les instances.

Notez que la sélection de type d'instance basée sur des attributs ne permet pas de sélectionner les groupes de capacités à partir desquels allouer la flotte ; c'est la tâche des stratégies d'allocation.

Si vous spécifiez une stratégie d'allocation, la flotte EC2 lance des instances conformément à la stratégie d'allocation spécifiée.

- Pour les instances Spot, la sélection de type d'instance basée sur des attributs prend en charge les stratégies d'allocation `price-capacity-optimized`, `capacity-optimized` et `lowest-price`. Notez que nous ne recommandons pas la stratégie d'allocation `lowest-price` ponctuelle, car c'est elle qui présente le risque d'interruption le plus élevé pour vos instances ponctuelles.
- Pour les instances à la demande, la sélection de type d'instance basée sur des attributs prend en charge les stratégies d'allocation `lowest-price`.
- S'il n'y a pas de capacité pour les types d'instance avec des attributs d'instance spécifiés, aucune instance ne peut être lancée et la flotte renvoie une erreur.

Protection des prix

La protection des prix est une fonction qui empêche votre flotte EC2 d'utiliser des types d'instance que vous considéreriez trop chers même s'ils correspondent aux attributs que vous avez spécifiés. Pour utiliser la protection des prix, vous devez définir un seuil de prix. Ensuite, lorsqu'Amazon EC2 sélectionne des types d'instances avec vos attributs, il exclut les types d'instances dont le prix est supérieur à votre seuil.

Amazon EC2 calcule le seuil de prix de la manière suivante :

- Amazon EC2 identifie d'abord le type d'instance le moins cher parmi ceux qui correspondent à vos attributs.
- Amazon EC2 prend ensuite la valeur (exprimée en pourcentage) que vous avez spécifiée pour le paramètre de protection des prix et la multiplie par le prix du type d'instance identifié. Le résultat est le prix qui est utilisé comme seuil de prix.

Il existe des seuils de prix distincts pour les instances à la demande et les instances ponctuelles.

Lorsque vous créez un parc avec sélection du type d'instance basée sur les attributs, la protection des prix est activée par défaut. Vous pouvez conserver les valeurs par défaut ou définir les vôtres.

Vous pouvez également désactiver la protection des prix. Pour n'indiquer aucun seuil de protection des prix, spécifiez une valeur en pourcentage élevée, telle que 999999.

Rubriques

- [Comment est identifié le type d'instance le moins cher](#)
- [Protection du prix des instances à la demande](#)

- [Protection des prix des instances Spot](#)
- [Spécifiez le seuil de protection des prix](#)

Comment est identifié le type d'instance le moins cher

Amazon EC2 détermine le prix sur lequel baser le seuil de prix en identifiant le type d'instance dont le prix est le plus bas parmi celles qui correspondent aux attributs que vous avez spécifiés. Pour ce faire, il procède de la manière suivante :

- Il examine d'abord les types d'instances C, M ou R de la génération actuelle qui correspondent à vos attributs. S'il trouve des correspondances, il identifie le type d'instance le moins cher.
- S'il n'y a pas de correspondance, il examine ensuite tous les types d'instances de la génération actuelle qui correspondent à vos attributs. S'il trouve des correspondances, il identifie le type d'instance le moins cher.
- S'il n'y a pas de correspondance, il examine ensuite tous les types d'instances de la génération précédente qui correspondent à vos attributs et identifie le type d'instance le moins cher.

Protection du prix des instances à la demande

Le seuil de protection des prix pour les types d'instances à la demande est calculé sous la forme d'un pourcentage supérieur au type d'instance à la demande le moins cher identifié (`OnDemandMaxPricePercentageOverLowestPrice`). Vous spécifiez le pourcentage supérieur que vous êtes prêt à payer. Si vous ne spécifiez pas ce paramètre, la valeur par défaut de 20 est utilisée pour calculer un seuil de protection des prix supérieur de 20 % au prix identifié.

Par exemple, si le prix de l'instance On-Demand identifié est 0.4271, et que vous le spécifiez 25, le seuil de prix est supérieur de 25 % à 0.4271. Il est calculé comme suit : $0.4271 * 1.25 = 0.533875$. Le prix calculé est le montant maximum que vous êtes prêt à payer pour les instances à la demande et, dans cet exemple, Amazon EC2 exclura tous les types d'instances à la demande dont le coût est supérieur à 0.533875.

Protection des prix des instances Spot

Par défaut, Amazon EC2 applique automatiquement une protection optimale du prix des instances Spot afin de sélectionner de manière cohérente un large éventail de types d'instances. Vous pouvez également définir vous-même la protection des prix manuellement. Toutefois, laisser Amazon EC2 le faire à votre place peut améliorer les chances que votre capacité Spot soit atteinte.

Vous pouvez définir manuellement la protection des prix à l'aide de l'une des options suivantes. Si vous définissez manuellement la protection des prix, nous vous recommandons d'utiliser la première option.

- Pourcentage du type d'instance à la demande le moins cher identifié
[MaxSpotPriceAsPercentageOfOptimalOnDemandPrice]

Par exemple, si le prix du type d'instance On-Demand identifié est 0.4271, et que vous le spécifiez 60, le seuil de prix est de 60 % de 0.4271. Il est calculé comme suit : $0.4271 * 0.60 = 0.25626$. Le prix calculé est le montant maximum que vous êtes prêt à payer pour les instances Spot et, dans cet exemple, Amazon EC2 exclura tous les types d'instances Spot dont le coût est supérieur à 0.25626.

- Un pourcentage supérieur au type d'instance Spot le moins cher identifié
[SpotMaxPricePercentageOverLowestPrice]

Par exemple, si le prix du type d'instance Spot identifié est 0.1808, et que vous le spécifiez 25, le seuil de prix est supérieur de 25 % à 0.1808. Il est calculé comme suit : $0.1808 * 1.25 = 0.226$. Le prix calculé est le montant maximum que vous êtes prêt à payer pour les instances Spot et, dans cet exemple, Amazon EC2 exclura tous les types d'instances Spot dont le coût est supérieur à 0.266. Nous vous déconseillons d'utiliser ce paramètre car les prix au comptant peuvent fluctuer et, par conséquent, votre seuil de protection contre les prix peut également fluctuer.

Spécifiez le seuil de protection des prix

Pour spécifier le seuil de protection des prix

Lors de la création de la flotte EC2, configurez la flotte pour la sélection du type d'instance basée sur des attributs, puis procédez comme suit :

- Pour spécifier le seuil de protection des prix de l'instance à la demande, dans le fichier de configuration JSON, dans la structure InstanceRequirements, pour OnDemandMaxPricePercentageOverLowestPrice, saisissez le seuil de protection des prix sous forme de pourcentage.
- Pour spécifier le seuil de protection des prix des instances Spot, dans le fichier de configuration JSON, dans la InstanceRequirements structure, spécifiez l'un des paramètres suivants :
 - Pour MaxSpotPriceAsPercentageOfOptimalOnDemandPrice, entrez le seuil de protection des prix sous forme de pourcentage.

- `SpotMaxPricePercentageOverLowestPrice`, entrez le seuil de protection des prix sous forme de pourcentage.

Pour plus d'informations sur la création de flottes, veuillez consulter [Créer une flotte EC2 avec une sélection de type d'instance basée sur des attributs](#).

Note

Lors de la création de la flotte EC2, si vous définissez `TargetCapacityUnitType` sur `vcpu` ou `memory-mib`, le seuil de protection des prix est appliqué en fonction du prix par vCPU ou par mémoire au lieu du prix par instance.

Considérations

- Vous pouvez spécifier des types d'instance ou des attributs d'instance dans une flotte EC2, mais pas les deux en même temps.

Lorsque vous utilisez la CLI, les remplacements du modèle de lancement remplacent le modèle de lancement. Par exemple, si le modèle de lancement contient un type d'instance et que le remplacement du modèle de lancement contient des attributs d'instance, les instances identifiées par les attributs d'instance remplaceront le type d'instance dans le modèle de lancement.

- Lorsque vous utilisez la CLI, si vous spécifiez des attributs d'instance comme remplacements, vous ne pouvez pas non plus spécifier de pondérations ou de priorités.
- Vous pouvez spécifier un maximum de quatre structures `InstanceRequirements` dans une configuration de demande.

Créer une flotte EC2 avec une sélection de type d'instance basée sur des attributs

Vous pouvez configurer une flotte pour qu'elle utilise la sélection de type d'instance basée sur des attributs à l'aide de la AWS CLI.

Pour créer une flotte EC2 avec une sélection de type d'instance basée sur des attributs (AWS CLI)

Utilisez la commande [create-fleet](#) (AWS CLI) pour créer une flotte EC2. Spécifiez la configuration de flotte dans un fichier JSON.

```
aws ec2 create-fleet \
```

```
--region us-east-1 \  
--cli-input-json file://file_name.json
```

Exemple de fichier *file_name*.json

L'exemple suivant contient les paramètres qui configurent une flotte EC2 afin qu'elle utilise la sélection de type d'instance basée sur des attributs et est suivi d'une explication textuelle.

```
{  
  "SpotOptions": {  
    "AllocationStrategy": "price-capacity-optimized"  
  },  
  "LaunchTemplateConfigs": [{  
    "LaunchTemplateSpecification": {  
      "LaunchTemplateName": "my-launch-template",  
      "Version": "1"  
    },  
    "Overrides": [{  
      "InstanceRequirements": {  
        "VCpuCount": {  
          "Min": 2  
        },  
        "MemoryMiB": {  
          "Min": 4  
        }  
      }  
    }  
  ]  
},  
  "TargetCapacitySpecification": {  
    "TotalTargetCapacity": 20,  
    "DefaultTargetCapacityType": "spot"  
  },  
  "Type": "instant"  
}
```

Les attributs de sélection du type d'instance basé sur des attributs sont spécifiés dans la structure InstanceRequirements. Dans cet exemple, deux attributs sont spécifiés :

- VCpuCount : au moins 2 vCPU sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.
- MemoryMiB : au moins 4 Mio de mémoire sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.

Tout type d'instance doté d'au moins 2 vCPU et d'au moins 4 Mio de mémoire sera identifié.

Toutefois, la protection des prix et la stratégie d'allocation peuvent exclure certains types d'instances lorsque [la flotte EC2 alloue la flotte](#).

Pour obtenir une liste et une description de tous les attributs possibles que vous pouvez spécifier, consultez le [InstanceRequirements](#) manuel Amazon EC2 API Reference.

Note

Lorsque InstanceRequirements est inclus dans la configuration de la flotte, InstanceType et WeightedCapacity doivent être exclus. Ils ne peuvent pas déterminer la configuration de la flotte en même temps que les attributs d'instance.

Le JSON contient également la configuration de flotte suivante :

- "AllocationStrategy": "*price-capacity-optimized*" : la stratégie d'allocation des instances Spot de la flotte.
- "LaunchTemplateName": "*my-launch-template*", "Version": "*1*" : le modèle de lancement contient certaines informations de configuration d'instance, mais si des types d'instance sont spécifiés, ils seront remplacés par les attributs spécifiés dans InstanceRequirements.
- "TotalTargetCapacity": *20* : la capacité cible est de 20 instances Spot.
- "DefaultTargetCapacityType": "*spot*" : la capacité par défaut est celle des instances Spot.
- "Type": "*instant*" : le type de demande pour la flotte est instant.

Exemples de configurations valides et non valides

Si vous utilisez le AWS CLI pour créer une flotte EC2, vous devez vous assurer que la configuration de votre flotte est valide. Les exemples suivants illustrent les configurations valides et non valides.

Les configurations sont considérées comme non valides lorsqu'elles contiennent les éléments suivants :

- Une seule structure Overrides avec InstanceRequirements et InstanceType
- Deux structures Overrides, l'une avec InstanceRequirements et l'autre avec InstanceType
- Deux structures InstanceRequirements avec des valeurs d'attributs qui se chevauchent au sein du même LaunchTemplateSpecification

Exemples de configuration

- [Configuration valide : modèle de lancement unique avec remplacements](#)
- [Configuration valide : modèle de lancement unique avec plusieurs InstanceRequirements](#)
- [Configuration valide : deux modèles de lancement, chacun avec des remplacements](#)
- [Configuration valide : uniquement InstanceRequirements est spécifié, les valeurs d'attribut ne se chevauchent pas](#)
- [Configuration non valide : les Overrides contiennent InstanceRequirements et InstanceType](#)
- [Configuration non valide : deux Overrides contiennent InstanceRequirements et InstanceType](#)
- [Configuration non valide : chevauchement des valeurs d'attribut](#)

Configuration valide : modèle de lancement unique avec remplacements

La configuration suivante est valide. Elle contient un modèle de lancement et une structure Overrides contenant une structure InstanceRequirements. Vous trouverez ci-dessous une explication textuelle de l'exemple de configuration.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "My-launch-template",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceRequirements": {
            "VCpuCount": {
              "Min": 2,
              "Max": 8
            },
            "MemoryMib": {
              "Min": 0,
              "Max": 10240
            },
            "MemoryGiBPerVCpu": {
              "Max": 10000
            },
            "RequireHibernateSupport": true
          }
        }
      ]
    }
  ]
}
```

```
    }
  ]
}
],
"TargetCapacitySpecification": {
  "TotalTargetCapacity": 5000,
  "DefaultTargetCapacityType": "spot",
  "TargetCapacityUnitType": "vcpu"
}
}
```

InstanceRequirements

Pour utiliser la sélection d'instance basée sur les attributs, vous devez inclure la structure `InstanceRequirements` dans votre configuration de flotte et spécifier les attributs souhaités pour les instances de la flotte.

Dans l'exemple précédent, les attributs d'instance suivants sont spécifiés :

- `VCpuCount` : les types d'instances doivent comporter au minimum 2 et au maximum 8 vCPU.
- `MemoryMiB` : les types d'instance doivent disposer d'un maximum de 10 240 Mio de mémoire. Un minimum de 0 indique qu'il n'y a pas de limite minimale.
- `MemoryGiBPerVCpu` : les types d'instance doivent disposer d'un maximum de 10 000 Gio de mémoire par vCPU. Le paramètre `Min` est facultatif. En l'omettant, vous n'indiquez aucune limite minimale.

TargetCapacityUnitType

Le paramètre `TargetCapacityUnitType` spécifie l'unité de la capacité cible. Dans cet exemple, la capacité cible est 5000 et le type d'unité de capacité cible est `vcpu`, qui spécifient ensemble une capacité cible souhaitée de 5 000 vCPU. La flotte EC2 lancera suffisamment d'instances pour que le nombre total de vCPU dans la flotte soit de 5 000.

Configuration valide : modèle de lancement unique avec plusieurs `InstanceRequirements`

La configuration suivante est valide. Elle contient un modèle de lancement et une structure `Overrides` contenant deux structures `InstanceRequirements`. Les attributs spécifiés dans `InstanceRequirements` sont valides car les valeurs ne se chevauchent pas. La première structure

InstanceRequirements spécifie une VCpuCount de 0 à 2 vCPU, tandis que la seconde structure InstanceRequirements spécifie 4 à 8 vCPU.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "MyLaunchTemplate",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceRequirements": {
            "VCpuCount": {
              "Min": 0,
              "Max": 2
            },
            "MemoryMiB": {
              "Min": 0
            }
          }
        },
        {
          "InstanceRequirements": {
            "VCpuCount": {
              "Min": 4,
              "Max": 8
            },
            "MemoryMiB": {
              "Min": 0
            }
          }
        }
      ]
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 1,
    "DefaultTargetCapacityType": "spot"
  }
}
```

Configuration valide : deux modèles de lancement, chacun avec des remplacements

La configuration suivante est valide. Elle contient deux modèles de lancement, chacun contenant une structure `Overrides` contenant une structure `InstanceRequirements`. Cette configuration est utile pour la prise en charge des architectures arm et x86 au sein de la même flotte.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "armLaunchTemplate",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceRequirements": {
            "VCpuCount": {
              "Min": 0,
              "Max": 2
            },
            "MemoryMiB": {
              "Min": 0
            }
          }
        }
      ],
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "x86LaunchTemplate",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceRequirements": {
            "VCpuCount": {
              "Min": 0,
              "Max": 2
            },
            "MemoryMiB": {
              "Min": 0
            }
          }
        }
      ]
    }
  ]
}
```

```
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 1,
    "DefaultTargetCapacityType": "spot"
  }
}
```

Configuration valide : uniquement **InstanceRequirements** est spécifié, les valeurs d'attribut ne se chevauchent pas

La configuration suivante est valide. Elle contient deux structures `LaunchTemplateSpecification`, chacune avec un modèle de lancement et une structure `Overrides` contenant une structure `InstanceRequirements`. Les attributs spécifiés dans `InstanceRequirements` sont valides car les valeurs ne se chevauchent pas. La première structure `InstanceRequirements` spécifie une `VCpuCount` de 0 à 2 vCPU, tandis que la seconde structure `InstanceRequirements` spécifie 4 à 8 vCPU.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "MyLaunchTemplate",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceRequirements": {
            "VCpuCount": {
              "Min": 0,
              "Max": 2
            },
            "MemoryMiB": {
              "Min": 0
            }
          }
        }
      ]
    },
    {
      "LaunchTemplateSpecification": {
```

```

        "LaunchTemplateName": "MyOtherLaunchTemplate",
        "Version": "1"
    },
    "Overrides": [
    {
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 4,
                "Max": 8
            },
            "MemoryMiB": {
                "Min": 0
            }
        }
    }
    ]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 1,
    "DefaultTargetCapacityType": "spot"
}
}
}

```

Configuration non valide : les **Overrides** contiennent **InstanceRequirements** et **InstanceType**

La configuration suivante n'est pas valide. La structure `Overrides` contient à la fois `InstanceRequirements` et `InstanceType`. Pour les `Overrides`, vous pouvez spécifier `InstanceRequirements` ou `InstanceType`, mais pas les deux.

```

{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "MyLaunchTemplate",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,

```

```

        "Max": 2
      },
      "MemoryMiB": {
        "Min": 0
      }
    },
    {
      "InstanceType": "m5.large"
    }
  ]
}
],
"TargetCapacitySpecification": {
  "TotalTargetCapacity": 1,
  "DefaultTargetCapacityType": "spot"
}
}
}

```

Configuration non valide : deux **Overrides** contiennent **InstanceRequirements** et **InstanceType**

La configuration suivante n'est pas valide. Les structures **Overrides** contiennent à la fois **InstanceRequirements** et **InstanceType**. Vous pouvez spécifier **InstanceRequirements** ou **InstanceType**, mais pas les deux, même s'ils se trouvent dans différentes structures **Overrides**.

```

{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "MyLaunchTemplate",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceRequirements": {
            "VCpuCount": {
              "Min": 0,
              "Max": 2
            },
            "MemoryMiB": {
              "Min": 0
            }
          }
        }
      ]
    }
  ]
}

```

```

    }
  }
}
],
},
{
  "LaunchTemplateSpecification": {
    "LaunchTemplateName": "MyOtherLaunchTemplate",
    "Version": "1"
  },
  "Overrides": [
    {
      "InstanceType": "m5.large"
    }
  ]
}
],
"TargetCapacitySpecification": {
  "TotalTargetCapacity": 1,
  "DefaultTargetCapacityType": "spot"
}
}
}

```

Configuration non valide : chevauchement des valeurs d'attribut

La configuration suivante n'est pas valide. Les deux structures `InstanceRequirements` contiennent chacune `"VCpuCount": {"Min": 0, "Max": 2}`. Les valeurs de ces attributs se chevauchent, ce qui entraîne des groupes de capacités en double.

```

{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "MyLaunchTemplate",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceRequirements": {
            "VCpuCount": {
              "Min": 0,
              "Max": 2
            }
          }
        }
      ]
    }
  ]
}

```



```
--region us-east-1 \  
--generate-cli-skeleton input > attributes.json
```

Sortie attendue

```
{  
  "DryRun": true,  
  "ArchitectureTypes": [  
    "i386"  
  ],  
  "VirtualizationTypes": [  
    "hvm"  
  ],  
  "InstanceRequirements": {  
    "VCpuCount": {  
      "Min": 0,  
      "Max": 0  
    },  
    "MemoryMiB": {  
      "Min": 0,  
      "Max": 0  
    },  
    "CpuManufacturers": [  
      "intel"  
    ],  
    "MemoryGiBPerVCpu": {  
      "Min": 0.0,  
      "Max": 0.0  
    },  
    "ExcludedInstanceTypes": [  
      ""  
    ],  
    "InstanceGenerations": [  
      "current"  
    ],  
    "SpotMaxPricePercentageOverLowestPrice": 0,  
    "OnDemandMaxPricePercentageOverLowestPrice": 0,  
    "BareMetal": "included",  
    "BurstablePerformance": "included",  
    "RequireHibernateSupport": true,  
    "NetworkInterfaceCount": {  
      "Min": 0,  
      "Max": 0  
    }  
  }  
}
```

```
    },
    "LocalStorage": "included",
    "LocalStorageTypes": [
      "hdd"
    ],
    "TotalLocalStorageGB": {
      "Min": 0.0,
      "Max": 0.0
    },
    "BaselineEbsBandwidthMbps": {
      "Min": 0,
      "Max": 0
    },
    "AcceleratorTypes": [
      "gpu"
    ],
    "AcceleratorCount": {
      "Min": 0,
      "Max": 0
    },
    "AcceleratorManufacturers": [
      "nvidia"
    ],
    "AcceleratorNames": [
      "a100"
    ],
    "AcceleratorTotalMemoryMiB": {
      "Min": 0,
      "Max": 0
    },
    "NetworkBandwidthGbps": {
      "Min": 0.0,
      "Max": 0.0
    },
    "AllowedInstanceTypes": [
      ""
    ]
  },
  "MaxResults": 0,
  "NextToken": ""
}
```

2. Créez un fichier de configuration JSON à l'aide de la sortie de l'étape précédente et configurez-le comme suit :

Note

Vous devez fournir des valeurs pour `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` et `MemoryMiB`. Vous pouvez omettre les autres attributs. Lorsqu'ils sont omis, les valeurs par défaut sont utilisées.

Pour obtenir une description de chaque attribut et de leurs valeurs par défaut, consultez [get-instance-types-from-instance-requirements](#) dans la Référence des commandes en ligne Amazon EC2.

- a. Pour `ArchitectureTypes`, spécifiez un ou plusieurs types d'architecture de processeur.
 - b. Pour `VirtualizationTypes`, spécifiez un ou plusieurs types de virtualisation.
 - c. Pour `VCpuCount`, spécifiez le nombre minimum et maximum de vCPU. Pour ne spécifier aucune limite minimale, pour `Min`, spécifiez `0`. Pour ne spécifier aucune limite maximale, omettez le paramètre `Max`.
 - d. Pour `MemoryMiB`, spécifiez la quantité minimale et maximale de mémoire en Mio. Pour ne spécifier aucune limite minimale, pour `Min`, spécifiez `0`. Pour ne spécifier aucune limite maximale, omettez le paramètre `Max`.
 - e. Vous pouvez éventuellement spécifier un ou plusieurs autres attributs pour limiter davantage la liste des types d'instance renvoyés.
3. Pour afficher un aperçu des types d'instance qui possèdent les attributs que vous avez spécifiés dans le fichier JSON, utilisez la commande [get-instance-types-from-instance-requirements](#) et spécifiez le nom et le chemin d'accès à votre fichier JSON à l'aide du paramètre `--cli-input-json`. Vous pouvez éventuellement formater la sortie pour qu'elle apparaisse dans un format de tableau.

```
aws ec2 get-instance-types-from-instance-requirements \  
  --cli-input-json file://attributes.json \  
  --output table
```

Fichier *attributes.json* d'exemple

Dans cet exemple, les attributs requis sont inclus dans le fichier JSON. Ils sont `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` et `MemoryMiB`. En outre,

l'attribut facultatif InstanceGenerations est également inclus. Notez que pour MemoryMiB, la valeur Max peut être omise pour indiquer qu'aucune limite n'est applicable.

```
{
  "ArchitectureTypes": [
    "x86_64"
  ],
  "VirtualizationTypes": [
    "hvm"
  ],
  "InstanceRequirements": {
    "VCpuCount": {
      "Min": 4,
      "Max": 6
    },
    "MemoryMiB": {
      "Min": 2048
    },
    "InstanceGenerations": [
      "current"
    ]
  }
}
```

Exemple de sortie

```
-----
|GetInstanceTypesFromInstanceRequirements|
+-----+
||           InstanceTypes           ||
|+-----+|
||           InstanceType           ||
|+-----+|
|| c4.xlarge                         ||
|| c5.xlarge                         ||
|| c5a.xlarge                        ||
|| c5ad.xlarge                       ||
|| c5d.xlarge                        ||
|| c5n.xlarge                        ||
|| d2.xlarge                         ||
|| ...                               ||
```

- Après avoir identifié les types d'instance qui répondent à vos besoins, prenez note des attributs d'instance que vous avez utilisés afin que vous puissiez les utiliser lors de la configuration de votre demande de flotte.

Configurer flotte EC2 pour la sauvegarde à la demande

En cas de besoin d'une mise à l'échelle imprévisible et urgente, par exemple pour un site web d'actualité qui doit être dimensionné à la hausse lors d'un événement d'actualité ou de la sortie d'un jeu majeur, nous vous recommandons de spécifier des types d'instance alternatifs pour vos instances à la demande, au cas où votre option préférée n'aurait pas une capacité disponible suffisante. Par exemple, vous pouvez préférer des Instances à la demande `c5.2xlarge`, mais si la capacité disponible est insuffisante, vous pouvez utiliser certaines instances `c4.2xlarge` lors des pics de charges. Dans ce cas, le Flotte EC2 tente d'assurer toute votre capacité cible en utilisant des instances `c5.2xlarge`, mais si la capacité est insuffisante, il lance automatiquement des instances `c4.2xlarge` pour assurer la capacité cible.

Rubriques

- [Hiérarchiser les types d'instance pour la capacité à la demande](#)
- [Utiliser réservations de capacité pour instances à la demande](#)

Hiérarchiser les types d'instance pour la capacité à la demande

Lorsque la flotte EC2 essaie de traiter l'affectation de capacité à la demande, elle lance par défaut le type d'instance dont le prix est le plus bas en premier. Si `AllocationStrategy` a pour valeur `prioritized`, le Flotte EC2 utilise la priorité pour déterminer quel type d'instance utiliser en premier afin de traiter l'affectation de capacité à la demande. La priorité est affectée au remplacement du modèle de lancement, et la priorité la plus élevée est lancée en premier.

Exemple : donner la priorité aux types d'instance

Dans cet exemple, vous configurez trois dérogations au modèle de lancement, chacune avec un type d'instance différent.

Le prix à la demande des types d'instance varie. Voici les types d'instance utilisés dans cet exemple, classés par ordre de prix, en commençant par le type d'instance le moins cher :

- `m4.large` : le moins cher
- `m5.large`

- `m5a.large`

Si vous n'utilisez pas la priorité pour déterminer l'ordre, la flotte remplit la capacité à la demande en commençant par le type d'instance le moins cher.

Toutefois, supposons que vous avez des instances réservées `m5.large` inutilisées que vous voulez utiliser en premier. Vous pouvez définir la priorité de remplacement du modèle de lancement afin que les types d'instance soient utilisés dans l'ordre de priorité, comme suit :

- `m5.large` : priorité 1
- `m4.large` : priorité 2
- `m5a.large` : priorité 3

Utiliser réservations de capacité pour instances à la demande

Les réservations de capacité à la demande vous permet de réserver de la capacité de calcul pour vos instances à la demande dans une zone de disponibilité spécifique, quelle que soit la durée. Vous pouvez configurer une flotte EC2 pour qu'elle utilise d'abord la réservations de capacité lors du lancement d'instances à la demande.

Les réservations de capacité sont configurées comme `open` ou `targeted`. La flotte EC2 peut lancer des instances à la demande, aussi bien dans des réservations de capacité `open` ou `targeted`, comme suit :

- Si une Réserve de capacité est `open`, les instances à la demande dont les attributs correspondent s'exécutent automatiquement dans la capacité réservée.
- Si la réservation de capacité est `targeted`, les instances doivent la cibler spécifiquement pour s'exécuter dans la capacité réservée. Cela est utile pour utiliser des réservations de capacité spécifiques ou pour contrôler quand utiliser des réservations de capacité spécifiques.

Si vous utilisez des réservations de capacité `targeted` dans votre flotte EC2, il doit y avoir suffisamment de réservations de capacité pour atteindre la capacité à la demande cible, sinon le lancement échoue. Afin éviter un échec de lancement, ajoutez plutôt les réserves de capacité `targeted` à un groupe de ressources, puis cibler le groupe de ressources. Le groupe de ressources n'a pas besoin d'avoir suffisamment de réservations de capacité ; s'il manque de réservations de capacité avant l'exécution de la capacité à la demande cible, la flotte peut lancer la capacité cible restante dans une capacité à la demande régulière.

Pour utiliser les réservations de capacité avec la flotte EC2

1. Configurer la flotte en tant que type `instant`. Vous ne pouvez pas utiliser les réservations de capacité pour les flottes d'autres types.
2. Configurer la stratégie d'utilisation des réservations de capacité en tant que `capacity-reservations-first`.
3. Dans le modèle de lancement, pour `Capacity reservation` (Réservation de capacité), choisissez entre `Open` (Ouvrir) et `Target by group` (Cible par groupe). Si vous choisissez `Target by group` (Cible par groupe), spécifiez l'ID du groupe de ressources réservations de capacité.

Lorsque la flotte tente de remplir la capacité à la demande, si elle constate que plusieurs groupes d'instances ont des réservations de capacité correspondantes inutilisées, elle détermine les groupes dans lesquels lancer les instances à la demande en fonction de la stratégie d'allocation à la demande (`lowest-price` ou `prioritized`).

Veillez consulter [Exemples de configuration d'une flotte EC2](#) pour obtenir des exemples sur la façon de configurer une flotte pour qu'elle utilise les réservations de capacité pour remplir la capacité à la demande, notamment les exemples 5 à 7.

Pour plus d'informations sur la configuration des réservations de capacité, consultez la rubrique [On-Demand Capacity Reservations](#) et la rubrique [On-Demand Capacity Reservation FAQs](#) (FAQ sur les réservations de capacité à la demande).

Rééquilibrage de la capacité

Vous pouvez configurer la flotte EC2 pour lancer un remplacement d'instance Spot lorsqu'Amazon EC2 émet une recommandation de rééquilibrage pour vous avertir qu'une instance Spot présente un risque d'interruption élevé. Le rééquilibrage de capacité vous permet de maintenir la disponibilité de la charge de travail en augmentant de manière proactive votre flotte avec une nouvelle instance Spot avant qu'une instance en cours d'exécution ne soit interrompue par Amazon EC2. Pour plus d'informations, consultez [Recommandations de rééquilibrage des instances EC2](#).

Pour configurer la flotte EC2 pour le lancement d'une instance Spot de remplacement, utilisez la commande [create-fleet](#) (AWS CLI) et les paramètres pertinents dans la structure `MaintenanceStrategies`. Pour plus d'informations, consultez l'[exemple de configuration de lancement](#).

Limites

- Le rééquilibrage de capacité est disponible uniquement pour les flottes de type `maintain`.
- Lorsque la flotte est en cours d'exécution, vous ne pouvez pas modifier le paramètre Rééquilibrage de capacité. Pour modifier le paramètre Rééquilibrage de capacité, vous devez supprimer la flotte et en créer un nouveau.

Options de configuration

La `ReplacementStrategy` pour la flotte EC2 prend en charge les deux valeurs suivantes :

`launch-before-terminate`

Amazon EC2 met fin aux instances Spot qui reçoivent une notification de rééquilibrage après le lancement de nouvelles instances Spot de remplacement. Quand vous spécifiez `launch-before-terminate`, vous devez également spécifier une valeur pour `termination-delay`. Une fois les nouvelles instances de remplacement lancées, Amazon EC2 attend la durée du `termination-delay`, puis résilie les anciennes instances. Pour `termination-delay`, le minimum est de 120 secondes (2 minutes) et le maximum est de 7 200 secondes (2 heures).

Nous vous recommandons d'utiliser `launch-before-terminate` uniquement si vous pouvez prédire la durée de la procédure d'arrêt de votre instance. Cela garantit que les anciennes instances ne sont résiliées qu'une fois les procédures d'arrêt terminées. Notez qu'Amazon EC2 peut interrompre les anciennes instances avec un avertissement de deux minutes avant le `termination-delay`.

Nous vous recommandons vivement de ne pas utiliser la stratégie d'allocation `lowest-price` combinée à `launch-before-terminate` afin d'éviter d'avoir des instances Spot de remplacement qui présentent un risque élevé d'interruption.

`launch`

Amazon EC2 lance des instances Spot de remplacement lorsqu'une notification de rééquilibrage est émise pour les instances Spot existantes. Amazon EC2 ne résilie pas les instances qui reçoivent une notification de rééquilibrage. Vous pouvez résilier les anciennes instances ou les laisser en cours d'exécution. Toutes les instances en cours d'exécution vous sont facturées.

Considérations

Si vous configurez une flotte EC2 pour le rééquilibrage de capacité, tenez compte des points suivants :

Fournissez autant de groupes de capacité Spot que possible dans la demande

Configurez votre flotte EC2 pour utiliser plusieurs types d'instance et zones de disponibilité. Cela permet de lancer des instances Spot dans divers groupes de capacité Spot. Pour plus d'informations, consultez [Soyez flexible en ce qui concerne les types d'instance et les zones de disponibilité](#).

Éviter un risque élevé d'interruption des instances Spot de remplacement

Vos instances Spot de remplacement peuvent présenter un risque élevé d'interruption si vous utilisez la stratégie d'allocation `lowest-price`. En effet, Amazon EC2 lancera toujours des instances dans le groupe le moins cher qui dispose de capacités disponibles à ce moment, même si vos instances Spot de remplacement risquent d'être interrompues peu après leur lancement. Pour éviter un risque élevé d'interruption, nous vous recommandons fortement de ne pas utiliser la stratégie d'allocation `lowest-price`, mais plutôt `capacity-optimized` ou `capacity-optimized-prioritized`. Ces stratégies garantissent que les instances Spot de remplacement sont lancées dans les groupes de capacité Spot optimaux et sont donc moins susceptibles d'être interrompues dans un proche avenir. Pour plus d'informations, consultez [Utiliser la stratégie d'allocation optimisée pour le prix et la capacité](#).

Amazon EC2 ne lancera une nouvelle instance que si la disponibilité est identique ou meilleure

L'un des objectifs du rééquilibrage de capacité est d'améliorer la disponibilité d'une instance Spot. Si une instance Spot existante reçoit une recommandation de rééquilibrage, Amazon EC2 ne lancera une nouvelle instance que si la nouvelle instance offre une disponibilité supérieure ou égale à celle de l'instance existante. Si le risque d'interruption d'une nouvelle instance est plus important que celui de l'instance existante, Amazon EC2 ne lancera pas de nouvelle instance. Amazon EC2 continuera toutefois à évaluer les groupes de capacité Spot et lancera une nouvelle instance si la disponibilité s'améliore.

Il est possible que votre instance existante soit interrompue sans qu'Amazon EC2 ne lance une nouvelle instance de manière proactive. Lorsque cela se produit, Amazon EC2 essaiera de lancer une nouvelle instance, que la nouvelle instance présente un risque d'interruption élevé ou non.

Le rééquilibrage de capacité n'augmente pas le taux d'interruption de votre instance Spot

Lorsque vous activez le rééquilibrage de la capacité, cette action n'augmente pas votre [Taux d'interruption d'instance Spot](#). (Le nombre d'instances Spot qui sont récupérées lorsqu'Amazon EC2 doit récupérer de l'espace. Toutefois, si le rééquilibrage de la capacité détecte une potentielle interruption d'instance, Amazon EC2 essaiera instantanément de lancer une nouvelle instance. En résultat, un nombre supérieur d'instances pourraient être remplacées, comparativement au scénario où vous attendriez qu'Amazon EC2 lance une nouvelle instance après l'interruption de l'instance à risque.

Bien que vous puissiez remplacer davantage d'instances lorsque le rééquilibrage de la capacité est activé, vous gagnerez à faire preuve de proactivité que de réactivité en disposant de plus de temps d'action avant l'interruption de vos instances. En général, après un [Avis d'interruption d'instance Spot](#), vous ne disposez que deux minutes pour arrêter correctement votre instance. Etant donné que le rééquilibrage de la capacité lance une nouvelle instance à l'avance, vous donnez aux processus existants de meilleures chances de se terminer sur votre instance à risque. Vous pouvez démarrer les procédures d'arrêt de votre instance et empêcher la planification de nouveaux travaux sur votre instance à risque. Vous pouvez également commencer à préparer l'instance nouvellement lancée afin de prendre le contrôle de l'application. Grâce au remplacement proactif de Capacity Rebalancing, vous bénéficiez d'une continuité.

À titre d'exemple théorique pour démontrer les risques et les avantages liés au rééquilibrage des capacités, considérez le scénario suivant :

- 14 h 00 : une recommandation de rééquilibrage est reçue pour l'instance-A, et Amazon EC2 essaie instantanément de lancer une Instance-B de remplacement, ce qui vous laisse le temps de démarrer vos procédures d'arrêt.*
- 14 h 30 — Une recommandation de rééquilibrage est reçue pour l'instance-B, remplacée par Instance-C, ce qui vous donne le temps de démarrer vos procédures d'arrêt. *
- 14 h 32 — Si le rééquilibrage de la capacité n'était pas activé, et si un avis d'interruption d'instance Spot avait été reçu à 14h32 pour l'instance-A, vous n'auriez disposé que de deux minutes pour agir. Cependant, l'instance-A aurait été en cours d'exécution jusqu'à ce moment.

* Si `launch-before-terminate` est spécifié, Amazon EC2 mettra fin à l'instance à risque après la mise en ligne de l'instance de remplacement.

Amazon EC2 peut lancer de nouvelles instances Spot de remplacement jusqu'à ce que la capacité exécutée représente le double de la capacité cible

Lorsqu'une flotte EC2 est configurée pour le rééquilibrage de capacité, la flotte tente de lancer une nouvelle instance Spot de remplacement pour chaque instance Spot qui reçoit une recommandation de rééquilibrage. Une fois qu'une instance Spot reçoit une recommandation de rééquilibrage, elle n'est plus comptabilisée dans la capacité exécutée. Selon la stratégie de remplacement, Amazon EC2 résilie l'instance après un délai de terminaison préconfiguré ou la laisse en cours d'exécution. Cela vous donne la possibilité d'effectuer des [actions de rééquilibrage](#) sur l'instance.

Si votre flotte atteint le double de sa capacité cible, il cesse de lancer de nouvelles instances de remplacement même si les instances de remplacement elles-mêmes reçoivent une recommandation de rééquilibrage.

Par exemple, vous créez une flotte EC2 avec une capacité cible de 100 instances Spot. Toutes les instances Spot reçoivent une recommandation de rééquilibrage, ce qui entraîne le lancement par Amazon EC2 de 100 instances Spot de remplacement. Cela augmente le nombre d'instances Spot exécutées à 200, soit le double de la capacité cible. Certaines instances de remplacement reçoivent une recommandation de rééquilibrage, mais aucune autre instance de remplacement n'est lancée car la flotte ne peut pas dépasser le double de sa capacité cible.

Notez que vous êtes facturé pour toutes les instances pendant qu'elles sont en cours d'exécution.

Nous vous recommandons de configurer la flotte EC2 afin qu'elle résilie les instances Spot qui reçoivent une recommandation de rééquilibrage

Si vous configurez votre flotte EC2 pour le rééquilibrage de capacité, nous vous recommandons de choisir `launch-before-terminate` avec un délai de résiliation approprié uniquement si vous pouvez prédire la durée de la procédure d'arrêt de votre instance. Cela garantit que les anciennes instances ne sont résiliées qu'une fois les procédures d'arrêt terminées.

Si vous choisissez de résilier vous-même les instances recommandées pour le rééquilibrage, nous vous recommandons de surveiller le signal de recommandation de rééquilibrage reçu par les instances Spot de la flotte. En surveillant le signal, vous pouvez effectuer rapidement des [actions de rééquilibrage](#) sur les instances concernées avant qu'Amazon EC2 ne les interrompe, puis vous pouvez les résilier manuellement. Si vous ne résiliez pas les instances, vous continuez à les payer pendant qu'elles sont en cours d'exécution. Amazon EC2 ne résilie pas automatiquement les instances qui reçoivent une recommandation de rééquilibrage.

Vous pouvez configurer des notifications à l'aide d'Amazon EventBridge ou des métadonnées d'instance. Pour plus d'informations, consultez [Surveiller les signaux de recommandation de rééquilibrage](#).

flotte EC2 ne prend pas en compte les instances qui reçoivent une recommandation de rééquilibrage lors du calcul de la capacité exécutée pendant la diminution ou l'augmentation

Si votre flotte EC2 est configuré pour le rééquilibrage de capacité et que vous modifiez la capacité cible pour qu'elle soit diminuée ou augmentée, la flotte ne comptabilise pas les instances marquées pour rééquilibrage dans le cadre de la capacité exécutée, comme suit :

- Mise à l'échelle horizontale : si vous diminuez la capacité cible souhaitée, Amazon EC2 résilie les instances qui ne sont pas marquées pour rééquilibrage tant que la capacité souhaitée n'est pas atteinte. Les instances marquées pour rééquilibrage ne sont pas prises en compte dans la capacité exécutée.

Par exemple, vous créez une flotte EC2 avec une capacité cible de 100 instances Spot. 10 instances reçoivent une recommandation de rééquilibrage, Amazon EC2 lance alors 10 nouvelles instances de remplacement, ce qui donne une capacité exécutée de 110 instances. Vous réduisez ensuite la capacité cible à 50 (mise à l'échelle horizontale), mais la capacité exécutée est en fait de 60 instances car les 10 instances marquées pour rééquilibrage ne sont pas résiliées par Amazon EC2. Vous devez résilier manuellement ces instances, ou vous pouvez les laisser en cours d'exécution.

- Montée en puissance : si vous augmentez la capacité cible souhaitée, Amazon EC2 lance de nouvelles instances tant que la capacité souhaitée n'est pas atteinte. Les instances marquées pour rééquilibrage ne sont pas prises en compte dans la capacité exécutée.

Par exemple, vous créez une flotte EC2 avec une capacité cible de 100 instances Spot. 10 instances reçoivent une recommandation de rééquilibrage, la flotte lance alors 10 nouvelles instances de remplacement, ce qui donne une capacité exécutée de 110 instances. Vous augmentez ensuite la capacité cible à 200 (augmentation), mais la capacité exécutée est en fait de 210 instances car les 10 instances marquées pour rééquilibrage ne sont pas comptabilisées par la flotte comme faisant partie de la capacité cible. Vous devez résilier manuellement ces instances, ou vous pouvez les laisser en cours d'exécution.

Remplacements du prix maximum

Chaque flotte EC2 peut inclure un prix maximum global ou utiliser la valeur par défaut (prix à la demande). Le flotte d'instances utilise ce prix comme prix maximum par défaut pour chacune de ses spécifications de lancement.

Si vous le souhaitez, vous pouvez également spécifier un prix maximum dans une ou plusieurs spécifications de lancement. Ce prix est propre à la spécification de lancement. Si une spécification de lancement comprend un prix spécifique, la flotte EC2 utilise ce prix maximum à la place du prix maximum global. Toute autre spécification de lancement qui ne comprend pas de prix maximum spécifique continue à utiliser le prix maximum global.

Contrôle des dépenses

Flotte EC2 arrête le lancement des instances une fois l'un des paramètres suivants atteints : le `TotalTargetCapacity` ou le `MaxTotalPrice` (montant maximum que vous êtes prêt à payer). Pour contrôler le montant payé par heure pour votre parc, vous pouvez spécifier `MaxTotalPrice`. Une fois le prix total atteint, flotte EC2 arrête de lancer des instances même si la capacité cible n'a pas été atteinte.

Les exemples suivants montrent deux manières de le faire. Dans le premier, flotte EC2 arrête de lancer des instances une fois la capacité cible atteinte. Dans le deuxième, Flotte EC2 arrête le lancement des instances une fois le montant maximum que vous êtes prêt à payer atteint (`MaxTotalPrice`).

Exemple : Arrêt du lancement des instances lorsque la capacité cible est atteinte

Prenons l'exemple d'une demande pour `m4.large` Instances à la demande, avec :

- Prix à la demande : 0,10 USD par heure
- `OnDemandTargetCapacity` : 10
- `MaxTotalPrice` : 1,50 USD

Flotte EC2 lance 10 Instances à la demande car le total de 1 USD (10 instances x 0,10 USD) ne dépasse pas le `MaxTotalPrice` de 1,50 USD pour Instances à la demande.

Exemple : Arrêt du lancement des instances lorsque le prix total maximum est atteint

Prenons l'exemple d'une demande pour `m4.large` Instances à la demande, avec :

- Prix à la demande : 0,10 USD par heure
- OnDemandTargetCapacity : 10
- MaxTotalPrice : 0,80 USD

Si flotte EC2 lance la capacité cible à la demande (10 instances à la demande), le coût total par heure est de 1 USD. Ce montant est supérieur à celui (0,80 USD) spécifié pour MaxTotalPrice pour Instances à la demande. Afin d'éviter de dépenser plus que vous le souhaitez, Flotte EC2 lance uniquement 8 Instances à la demande (ce qui est inférieur à la capacité cible à la demande) car le lancement d'instances supplémentaires dépasserait MaxTotalPrice pour Instances à la demande.

Pondération d'instance flotte EC2

Lorsque vous créez une flotte EC2, vous pouvez définir les unités de capacité que chaque type d'instance apporterait aux performances de votre application. Vous pouvez ensuite ajuster votre prix maximum pour chaque spécification de lancement en utilisant la pondération d'instance.

Par défaut, le prix que vous spécifiez représente le prix par heure d'instance. Lorsque vous utilisez la fonction de pondération d'instance, le prix que vous spécifiez correspond au prix par heure d'unité. Vous pouvez calculer le prix par heure d'unité en divisant le prix pour un type d'instance par le nombre d'unités qu'il représente. La flotte EC2 calcule le nombre d'instances à lancer en divisant la capacité cible par la pondération de l'instance. Si le résultat n'est pas un entier, la flotte d'instances l'arrondit à l'entier suivant afin que la taille de votre flotte ne soit pas inférieure à sa capacité cible. Le flotte d'instances peut sélectionner n'importe quel groupe indiqué dans votre spécification de lancement, même si la capacité des instances lancées dépasse la capacité cible demandée.

Le tableau suivant inclut des exemples de calcul afin de déterminer le prix par unité pour une flotte EC2 ayant une capacité cible de 10.

Type d'instance	Pondération de l'instance	Capacité cible	Nombre d'instances lancées	Prix par heure d'instance	Prix par heure d'unité
r3.xlarge	2	10	5 (10 divisé par 2)	0,05 USD	0,025 USD (0,05 divisé par 2)

Type d'instance	Pondération de l'instance	Capacité cible	Nombre d'instances lancées	Prix par heure d'instance	Prix par heure d'unité
r3.8xlarge	8	10	2 (10 divisé par 8, résultat arrondi)	0,10 USD	0,0125 USD (0,10 divisé par 8)

Utilisez la pondération d'instance de flotte EC2 comme suit, afin de mettre en service la capacité cible que vous voulez dans les groupes selon le prix par unité le plus bas au moment de l'exécution :

1. Définissez la capacité cible de votre flotte EC2 en instances (valeur par défaut) ou dans les unités de votre choix, par exemple les UC virtuelles, la mémoire, le stockage ou le débit.
2. Définissez le prix par unité.
3. Pour chaque spécification de lancement, spécifiez la pondération, à savoir le nombre d'unités que représente ce type d'instance par rapport à la capacité cible.

Exemple de pondération d'instance

Prenons l'exemple d'une demande de flotte EC2 avec la configuration suivante :

- Capacité cible de 24
- Spécification de lancement avec le type d'instance r3.2xlarge et une pondération de 6
- Spécification de lancement avec le type d'instance c3.xlarge et une pondération de 5

La pondération correspond au nombre d'unités du type d'instance par rapport à la capacité cible. Si la première spécification de lancement fournit le prix par unité le plus faible (prix pour r3.2xlarge par heure d'instance divisé par 6), le Flotte EC2 lance quatre de ces instances (24 divisé par 6).

Si la deuxième spécification de lancement fournit le prix par unité le plus bas (prix pour c3.xlarge par heure d'instance divisé par 5), le Flotte EC2 lance cinq de ces instances (24 divisé par 5, résultat arrondi).

Pondération d'instance et stratégie d'allocation

Prenons l'exemple d'une demande de flotte EC2 avec la configuration suivante :

- Capacité cible de 30 instances Spot
- Spécification de lancement avec le type d'instance `c3.2xlarge` et une pondération de 8
- Spécification de lancement avec le type d'instance `m3.xlarge` et une pondération de 8
- Spécification de lancement avec le type d'instance `r3.xlarge` et une pondération de 8

La flotte EC2 lancerait quatre instances (30 divisé par 8, résultat arrondi). Avec la stratégie `diversified`, le parc d'instances lance une instance dans chacun des trois groupes, et la quatrième instance dans l'un des trois groupes fournit le prix par unité le plus bas.

Travailler avec Flottes EC2

Pour commencer à utiliser une flotte EC2, vous créez une demande comprenant la capacité cible totale, une capacité à la demande, une capacité Spot, une ou plusieurs spécifications de lancement pour les instances et le prix maximum que vous êtes prêt à payer. La demande de flotte d'instances doit inclure un modèle de lancement qui définit les informations dont la flotte d'instances a besoin pour lancer une instance, par exemple une AMI, un type d'instance, un sous-réseau ou une zone de disponibilité, et un ou plusieurs groupes de sécurité. Vous pouvez spécifier des remplacements de spécification de lancement pour le type d'instance, le sous-réseau, la zone de disponibilité et le prix maximum que vous êtes prêt à payer, et vous pouvez affecter une capacité pondérée à chaque remplacement de spécification de lancement.

La flotte EC2 lance des instances à la demande lorsque la capacité requise est disponible, et il lance des instances Spot lorsque votre prix maximum dépasse le prix spot et que la capacité est disponible.

Si votre flotte d'instances inclut des instances Spot, Amazon EC2 tente de maintenir la capacité cible de votre flotte d'instances au fur et à mesure de l'évolution des prix Spot.

Une demande de Flotte EC2 de type `maintain` ou `request` reste active jusqu'à ce qu'elle arrive à expiration ou que vous la supprimiez. Lorsque vous supprimez une flotte de type `maintain` ou `request`, vous pouvez spécifier si la suppression résilie les instances de la flotte. Autrement, les instances à la demande s'exécutent jusqu'à ce que vous les résiliiez, et les instances Spot s'exécutent jusqu'à ce qu'elles soient interrompues ou que vous les résiliiez.

Table des matières

- [États des demandes flotte EC2](#)
- [Conditions préalables requises flotte EC2](#)
- [Vérifications de l'état par flotte EC2](#)
- [Générer un fichier de configuration JSON de flotte EC2](#)
- [Créer une flotte EC2](#)
- [Baliser une flotte EC2](#)
- [Décrire votre flotte EC2](#)
- [Modifier une flotte EC2](#)
- [Supprimer une flotte EC2](#)

États des demandes flotte EC2

Une demande de flotte EC2 peut avoir l'un des états suivants :

`submitted`

La demande de flotte EC2 est en cours d'évaluation et Amazon EC2 se prépare à lancer le nombre cible d'instances. La demande peut inclure instances à la demande, instances Spot, ou les deux. Si une requête dépasse les limites de votre flotte, elle est immédiatement supprimée.

`active`

La demande de flotte EC2 a été validée et Amazon EC2 tente de conserver le nombre cible d'instances en cours d'exécution. La demande conserve cet état jusqu'à ce qu'elle soit modifiée ou supprimée.

`modifying`

La demande de flotte EC2 est en cours de modification. La demande conserve cet état jusqu'à ce que la modification soit totalement traitée ou que la demande soit supprimée. Seul une flotte de type `maintain` peut être modifié. Cet état ne s'applique pas aux autres types de demandes.

`deleted_running`

La demande de flotte EC2 est supprimée et ne lance pas d'instances supplémentaires. Ses instances existantes continuent de s'exécuter jusqu'à ce qu'elles soient interrompues ou résiliées manuellement. La demande conserve cet état jusqu'à ce que toutes les instances soient interrompues ou mises hors service. Seule un Flotte EC2 de type `maintain` ou `request` peut avoir des instances en cours d'exécution après la suppression de la demande de Flotte EC2. Une

flotte instant supprimé avec des instances en cours d'exécution n'est pas pris en charge. Cet état ne s'applique pas aux flottes instant.

deleted_terminating

La demande de flotte EC2 est supprimée et ses instances sont résiliées. La demande conserve cet état jusqu'à ce que toutes les instances soient mises hors service.

deleted

La flotte EC2 est supprimé et n'a aucune instance en cours d'exécution. La demande est supprimée deux jours après la mise hors service de ses instances.

Conditions préalables requises flotte EC2

Pour créer une flotte EC2, les prérequis suivants doivent être en place :

- [Modèle de lancement](#)
- [Rôle lié à un service pour flotte EC2](#)
- [Octroyer un accès aux clés gérées par le client en vue de leur utilisation avec les AMI chiffrées et les instantanés EBS](#)
- [Autorisations pour les utilisateurs de la flotte d'instances EC2](#)

Modèle de lancement

Un modèle de lancement inclut des informations sur les instances à lancer, telles que le type d'instance, la zone de disponibilité et le prix maximum que vous êtes disposé à payer. Pour plus d'informations, consultez [Lancer une instance à partir d'un modèle de lancement](#).

Rôle lié à un service pour flotte EC2

Le rôle `AWSServiceRoleForEC2Fleet` accorde à la flotte EC2 l'autorisation de demander, lancer, résilier et étiqueter des instances en votre nom. Amazon EC2 utilise ce rôle lié à un service pour effectuer les actions suivantes :

- `ec2:RunInstances` – Lancer des instances
- `ec2:RequestSpotInstances` – Demander des Instances Spot.
- `ec2:TerminateInstances` – Résilier des instances
- `ec2:DescribeImages` – Décrire des AMI (Amazon Machine Image) pour les Instances Spot

- `ec2:DescribeInstanceStatus` – Décrire le statut des Instances Spot.
- `ec2:DescribeSubnets` – Décrire les sous-réseaux pour les Instances Spot.
- `ec2:CreateTags` – Ajoutez des balises aux Flotte EC2, aux instances et aux volumes.

Assurez-vous que ce rôle existe avant d'utiliser l'API AWS CLI ou une API pour créer une flotte EC2.

 Note

Un instant Flotte EC2 ne requiert pas ce rôle.

Pour créer le rôle, utilisez la console IAM comme suit.

Pour créer le `AWSServiceRoleForEC2Fleet` rôle pour EC2 Fleet

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.
3. Sur la page Sélectionner le type d'entité de confiance, procédez comme suit :
 - a. Pour Type d'entité de confiance, choisissez Service AWS .
 - b. Sous Cas d'utilisation, pour Service ou cas d'utilisation, choisissez EC2 - Fleet.

 Tip

Assurez-vous de choisir EC2 - Fleet. Si vous choisissez EC2, le cas d'utilisation EC2 - Fleet n'apparaît pas dans la liste des cas d'utilisation. Le cas d'utilisation d'EC2 - Fleet créera automatiquement une politique avec les autorisations IAM requises et suggérera le `AWSServiceRoleForEC2Fleetnom` du rôle.

- c. Choisissez Suivant.
4. Sur la page Ajouter des autorisations, sélectionnez Suivant.
 5. Sur la page Nommer, vérifier et créer, choisissez Créer un rôle.

Si vous n'avez plus besoin d'utiliser EC2 Fleet, nous vous recommandons de supprimer le `AWSServiceRoleForEC2Fleet` rôle. Après la suppression de ce rôle de votre compte, vous pouvez créer de nouveau le rôle si vous créez une autre flotte

Pour plus d'informations, consultez [Utilisation des rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Octroyer un accès aux clés gérées par le client en vue de leur utilisation avec les AMI chiffrées et les instantanés EBS

Si vous spécifiez une [AMI chiffrée](#) ou un instantané Amazon EBS chiffré dans votre flotte EC2 et que vous utilisez une AWS KMS clé pour le chiffrement, vous devez accorder au AWSServiceRoleForEC2Fleet rôle l'autorisation d'utiliser la clé gérée par le client afin qu'Amazon EC2 puisse lancer des instances en votre nom. Pour cela, vous devez ajouter une autorisation à la clé gérée par le client, comme indiqué dans la procédure suivante.

Lorsque vous définissez les autorisations, les octrois constituent une alternative aux politiques de clé. Pour plus d'informations, consultez les rubriques [Utilisation des octrois](#) et [Utilisation des politiques de clé dans AWS KMS](#) dans le Guide du développeur AWS Key Management Service .

Pour accorder au AWSServiceRoleForEC2Fleet rôle l'autorisation d'utiliser la clé gérée par le client

- Utilisez la commande [create-grant](#) pour ajouter une autorisation à la clé gérée par le client et pour spécifier le principal (le rôle AWSServiceRoleForEC2Fleet lié au service) autorisé à effectuer les opérations autorisées par l'autorisation. La clé gérée par le client est spécifiée par le paramètre `key-id` et l'ARN de la clé gérée par le client. Le principal est spécifié par le `grantee-principal` paramètre et l'ARN du rôle AWSServiceRoleForEC2Fleet lié au service.

```
aws kms create-grant \  
  --region us-east-1 \  
  --key-id arn:aws:kms:us-east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \  
  --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \  
  --operations "Decrypt" "Encrypt" "GenerateDataKey" \  
  "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom" \  
  "ReEncryptTo"
```

Autorisations pour les utilisateurs de la flotte d'instances EC2

Si vos utilisateurs sont appelés à créer ou à gérer une flotte EC2, veillez à leur accorder les autorisations nécessaires.

Pour créer une politique pour la flotte d'instances EC2

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Politiques (Politiques).
3. Sélectionnez Create policy (Créer une politique).
4. Sur la page Créer une stratégie, choisissez l'onglet JSON, remplacez le texte par le suivant, puis choisissez Examiner une stratégie.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles",
        "iam:PassRole",
        "iam:ListInstanceProfiles"
      ],
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

La fonction `ec2: *` accorde à un utilisateur l'autorisation d'appeler toutes les actions d'API Amazon EC2. Pour limiter les actions API Amazon EC2 susceptibles d'être effectuées par l'utilisateur, spécifiez celles qui sont autorisées.

L'utilisateur doit être autorisé à appeler l'action `iam:ListRoles` pour énumérer les rôles IAM existants, l'action `iam:PassRole` pour spécifier le rôle de flotte EC2 et l'action `iam:ListInstanceProfiles` pour énumérer les profils d'instance existants.

(Facultatif) Pour autoriser un utilisateur à créer des rôles ou des profils d'instances à l'aide de la console IAM, vous devez aussi ajouter les actions suivantes à la politique :

- `iam:AddRoleToInstanceProfile`
 - `iam:AttachRolePolicy`
 - `iam:CreateInstanceProfile`
 - `iam:CreateRole`
 - `iam:GetRole`
 - `iam:ListPolicies`
5. Sur la page Review Policy (Vérifier la stratégie), saisissez un nom et une description pour la stratégie, puis choisissez Create policy (Créer une stratégie).
6. Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :
- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .
 - Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.
 - Utilisateurs IAM :
 - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.
 - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Vérifications de l'état par flotte EC2

La flotte EC2 vérifie l'état de santé des instances de la flotte toutes les deux minutes. Le statut de l'état d'une instance est `healthy` ou `unhealthy`.

La flotte EC2 détermine le statut d'intégrité d'une instance en utilisant les contrôles de statut fournis par Amazon EC2. Une instance est déterminée comme `unhealthy` lorsque le contrôle du statut de l'instance ou de celui du système est `impaired` pendant trois vérifications consécutives de l'état d'intégrité. Pour plus d'informations, consultez [Contrôles de statut pour vos instances](#).

Vous pouvez configurer votre flotte pour qu'il remplace les instances Spot non saine. Après avoir paramétré `ReplaceUnhealthyInstances` sur `true`, une instance Spot est remplacée lorsqu'elle est signalée comme `unhealthy`. Notez que la taille de la flotte peut être inférieure à sa capacité cible pendant quelques minutes pendant le remplacement d'une instance Spot non saine.

Prérequis

- Le remplacement de la vérification de l'état est pris en charge uniquement pour les Flottes EC2 qui maintiennent une capacité cible (flottes de type `maintain`), pas avec des flottes de type `request` ou `instant`.
- Le remplacement de la vérification de l'état n'est pris en charge que pour instances Spot. Cette fonctionnalité n'est pas prise en charge pour instances à la demande.
- Vous pouvez configurer votre flotte EC2 pour qu'il remplace les instances non saines au moment de sa création uniquement.
- Les utilisateurs peuvent utiliser le remplacement lié à la surveillance de l'état seulement s'ils sont autorisés à appeler l'action `ec2:DescribeInstanceStatus`.

Pour configurer une flotte EC2 pour remplacer une instances Spot non saine

1. Suivez les étapes permettant de créer une flotte EC2. Pour plus d'informations, consultez [Créer une flotte EC2](#).
2. Pour configurer le parc de manière à remplacer les Instances Spot non saines, dans le fichier JSON, pour `ReplaceUnhealthyInstances`, entrez `true`.

Générer un fichier de configuration JSON de flotte EC2

Pour afficher la liste complète des paramètres de configuration de la flotte EC2, vous pouvez générer un fichier JSON. Pour obtenir une description de chaque paramètre, veuillez consulter [create-fleet](#) dans la référence des commandes AWS CLI .

Pour générer un fichier JSON avec tous les paramètres de flotte EC2 possibles à l'aide de la ligne de commande

- Utilisez la commande [create-fleet](#) (AWS CLI) et le paramètre `--generate-cli-skeleton` pour générer un fichier JSON de flotte EC2 et rediriger la sortie vers un fichier de sauvegarde.

```
aws ec2 create-fleet \
```

```
--generate-cli-skeleton input > ec2createfleet.json
```

Exemple de sortie

```
{
  "DryRun": true,
  "ClientToken": "",
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized",
    "MaintenanceStrategies": {
      "CapacityRebalance": {
        "ReplacementStrategy": "launch"
      }
    },
    "InstanceInterruptionBehavior": "hibernate",
    "InstancePoolsToUseCount": 0,
    "SingleInstanceType": true,
    "SingleAvailabilityZone": true,
    "MinTargetCapacity": 0,
    "MaxTotalPrice": ""
  },
  "OnDemandOptions": {
    "AllocationStrategy": "prioritized",
    "CapacityReservationOptions": {
      "UsageStrategy": "use-capacity-reservations-first"
    },
    "SingleInstanceType": true,
    "SingleAvailabilityZone": true,
    "MinTargetCapacity": 0,
    "MaxTotalPrice": ""
  },
  "ExcessCapacityTerminationPolicy": "termination",
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "",
        "LaunchTemplateName": "",
        "Version": ""
      },
      "Overrides": [
        {
          "InstanceType": "r5.metal",
          "MaxPrice": ""
        }
      ]
    }
  ]
}
```

```
"SubnetId": "",
"AvailabilityZone": "",
"WeightedCapacity": 0.0,
"Priority": 0.0,
"Placement": {
  "AvailabilityZone": "",
  "Affinity": "",
  "GroupName": "",
  "PartitionNumber": 0,
  "HostId": "",
  "Tenancy": "dedicated",
  "SpreadDomain": "",
  "HostResourceGroupArn": ""
},
"InstanceRequirements": {
  "VCpuCount": {
    "Min": 0,
    "Max": 0
  },
  "MemoryMiB": {
    "Min": 0,
    "Max": 0
  },
  "CpuManufacturers": [
    "amd"
  ],
  "MemoryGiBPerVCpu": {
    "Min": 0.0,
    "Max": 0.0
  },
  "ExcludedInstanceTypes": [
    ""
  ],
  "InstanceGenerations": [
    "previous"
  ],
  "SpotMaxPricePercentageOverLowestPrice": 0,
  "OnDemandMaxPricePercentageOverLowestPrice": 0,
  "BareMetal": "included",
  "BurstablePerformance": "required",
  "RequireHibernateSupport": true,
  "NetworkInterfaceCount": {
    "Min": 0,
    "Max": 0
  }
}
```

```
    },
    "LocalStorage": "excluded",
    "LocalStorageTypes": [
      "ssd"
    ],
    "TotalLocalStorageGB": {
      "Min": 0.0,
      "Max": 0.0
    },
    "BaselineEbsBandwidthMbps": {
      "Min": 0,
      "Max": 0
    },
    "AcceleratorTypes": [
      "inference"
    ],
    "AcceleratorCount": {
      "Min": 0,
      "Max": 0
    },
    "AcceleratorManufacturers": [
      "amd"
    ],
    "AcceleratorNames": [
      "a100"
    ],
    "AcceleratorTotalMemoryMiB": {
      "Min": 0,
      "Max": 0
    }
  }
}
],
"TargetCapacitySpecification": {
  "TotalTargetCapacity": 0,
  "OnDemandTargetCapacity": 0,
  "SpotTargetCapacity": 0,
  "DefaultTargetCapacityType": "on-demand",
  "TargetCapacityUnitType": "memory-mib"
},
"TerminateInstancesWithExpiration": true,
"Type": "instant",
```

```
"ValidFrom": "1970-01-01T00:00:00",
"ValidUntil": "1970-01-01T00:00:00",
"ReplaceUnhealthyInstances": true,
"TagSpecifications": [
  {
    "ResourceType": "fleet",
    "Tags": [
      {
        "Key": "",
        "Value": ""
      }
    ]
  }
],
"Context": ""
}
```

Créer une flotte EC2

Pour créer une flotte EC2, vous devez uniquement spécifier les paramètres suivants :

- `LaunchTemplateId` ou `LaunchTemplateName` : spécifie le modèle de lancement à utiliser (qui contient les paramètres des instances à lancer, tels que le type d'instance, la zone de disponibilité et le prix maximum que vous êtes disposé à payer)
- `TotalTargetCapacity` : spécifie la capacité cible totale de la flotte
- `DefaultTargetCapacityType` : indique si l'option d'achat par défaut est à la demande ou Spot

Vous pouvez spécifier plusieurs spécifications de lancement qui remplacent le modèle de lancement. Les spécifications de lancement peuvent varier en terme de type d'instance, zone de disponibilité, sous-réseau ou prix maximum, et elles peuvent inclure une capacité pondérée différente. Vous pouvez également spécifier les attributs qu'une instance doit posséder, et Amazon EC2 identifiera tous les types d'instance avec ces attributs. Pour plus d'informations, consultez [Sélection de type d'instance basée sur des attributs pour la flotte EC2](#).

Si vous ne spécifiez pas un paramètre, la flotte utilise la valeur par défaut.

Spécifiez les paramètres de flotte dans un fichier JSON. Pour plus d'informations, consultez [Générer un fichier de configuration JSON de flotte EC2](#).

Il n'existe actuellement aucune console compatible avec la création d'une flotte EC2.

Pour créer une flotte EC2 (AWS CLI)

- Utilisez la commande [create-fleet](#) (AWS CLI) pour créer une flotte EC2 et spécifier le fichier JSON qui contient les paramètres de configuration de la flotte.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Pour accéder à des exemples de fichiers de configuration, consultez [Exemples de configuration d'une flotte EC2](#).

Voici un exemple de sortie d'un parc d'instances du type `request` ou `maintain`.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Voici un exemple de sortie d'un parc d'instances du type `instant` qui a lancé la capacité cible.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
  ],
}
```

```
{
  "LaunchTemplateAndOverrides": {
    "LaunchTemplateSpecification": {
      "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
      "Version": "1"
    },
    "Overrides": {
      "InstanceType": "c4.large",
      "AvailabilityZone": "us-east-1a"
    }
  },
  "Lifecycle": "on-demand",
  "InstanceIds": [
    "i-5678901234abcdef0",
    "i-5432109876abcdef9"
  ]
}
```

Voici un exemple de sortie d'un parc d'instances du type `instant` qui a lancé une partie de la capacité cible avec les erreurs liées aux instances qui n'ont pas été lancées.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
```

```

    "LaunchTemplateAndOverrides": {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
        "Version": "1"
      },
      "Overrides": {
        "InstanceType": "c5.large",
        "AvailabilityZone": "us-east-1a"
      }
    },
    "Lifecycle": "on-demand",
    "InstanceIds": [
      "i-1234567890abcdef0",
      "i-9876543210abcdef9"
    ]
  ]
}

```

Voici un exemple de sortie d'un parc d'instances du type `instant` qui n'a lancé aucune instance.

```

{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        }
      }
    }
  ]
}

```

```
    },
    "Overrides": {
      "InstanceType": "c5.large",
      "AvailabilityZone": "us-east-1a",
    }
  },
  "Lifecycle": "on-demand",
  "ErrorCode": "InsufficientCapacity",
  "ErrorMessage": ""
},
],
"Instances": []
}
```

Baliser une flotte EC2

Pour vous aider à classer et à gérer vos demandes de flotte EC2, vous pouvez les baliser avec des métadonnées personnalisées. Vous pouvez affecter une balise à une demande de flotte EC2 lorsque vous la créez, ou après.

Lorsque vous balisez une demande de flotte, les instances et les volumes lancés par la flotte ne sont pas balisés automatiquement. Vous devez baliser explicitement les instances et les volumes lancés par la flotte. Vous pouvez choisir d'affecter des balises uniquement à la demande de flotte, ou uniquement aux instances lancées par la flotte, ou uniquement aux volumes attachés aux instances lancées par la flotte, ou aux trois.

Note

Pour les types de parc `instant`, vous pouvez baliser les volumes attachés à Instances à la demande et Instances Spot. Pour les types de parc `request` ou `maintain`, vous pouvez uniquement baliser les volumes attachés à Instances à la demande.

Pour plus d'informations sur le fonctionnement des balises, consultez [Baliser vos ressources Amazon EC2](#).

Prérequis

Octroyez à l'utilisateur l'autorisation de baliser les ressources. Pour plus d'informations, consultez [Exemple : Baliser des ressources](#).

Pour accorder à un utilisateur l'autorisation de baliser les ressources

Créez une politique IAM qui inclut les éléments suivants :

- L'action `ec2:CreateTags`. Celle-ci accorde à l'utilisateur l'autorisation de créer des balises.
- L'action `ec2:CreateFleet`. Celle-ci accorde à l'utilisateur l'autorisation de créer une demande flotte EC2.
- Pour `Resource`, nous vous recommandons de spécifier `"*"`. Cela permet aux utilisateurs de baliser tous les types de ressources.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "TagEC2FleetRequest",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:CreateFleet"
      ],
      "Resource": "*"
    }
  ]
}
```

Important

Actuellement, nous ne prenons pas en charge les autorisations de niveau ressource pour la ressource `create-fleet`. Si vous spécifiez `create-fleet` en tant que ressource, vous recevrez une exception de non-autorisation lorsque vous tenterez de baliser le parc. L'exemple suivant illustre comment ne pas définir la stratégie.

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateTags",
    "ec2:CreateFleet"
  ],
  "Resource": "arn:aws:ec2:us-east-1:111122223333:create-fleet/*"
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Pour baliser une nouvelle demande flotte EC2

Pour baliser une demande de Flotte EC2 lorsque vous la créez, spécifiez la paire clé-valeur dans le [fichier JSON](#) utilisé pour créer le parc d'instances. La valeur pour `ResourceType` doit être `fleet`. Si vous spécifiez une autre valeur, la demande de flotte d'instances échoue.

Pour baliser des instances et des volumes lancés par une flotte EC2

Pour baliser des instances et des volumes lorsqu'ils sont lancés par le parc d'instances, spécifiez les balises dans le [modèle de lancement](#) référencé dans la demande Flotte EC2.

Note

Vous ne pouvez pas baliser les volumes attachés à Instances Spot qui sont lancés par un type de parc `request` ou `maintain`.

Pour étiqueter une demande de flotte EC2, une instance et un volume existants (AWS CLI)

Utilisez la commande [create-tags](#) pour baliser les ressources existantes.

```
aws ec2 create-tags \
```

```
--resources fleet-12a34b55-67cd-8ef9-  
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \  
--tags Key=purpose,Value=test
```

Décrire votre flotte EC2

Vous pouvez décrire la configuration, les instances et l'historique des événements de votre flotte EC2.

Pour décrire vos flottes EC2 (AWS CLI)

Utilisez la commande [describe-fleets](#) suivante pour décrire vos Flottes EC2 :

```
aws ec2 describe-fleets
```

Important

Si une flotte est de type `instant`, vous devez spécifier son ID, sinon il n'apparaît pas dans la réponse. Inclure `--fleet-ids` comme suit :

```
aws ec2 describe-fleets --fleet-ids fleet-8a22eee4-f489-ab02-06b8-832a7EXAMPLE
```

Exemple de sortie

```
{  
  "Fleets": [  
    {  
      "ActivityStatus": "fulfilled",  
      "CreateTime": "2022-02-09T03:35:52+00:00",  
      "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",  
      "FleetState": "active",  
      "ExcessCapacityTerminationPolicy": "termination",  
      "FulfilledCapacity": 2.0,  
      "FulfilledOnDemandCapacity": 0.0,  
      "LaunchTemplateConfigs": [  
        {  
          "LaunchTemplateSpecification": {  
            "LaunchTemplateName": "my-launch-template",  
            "Version": "$Latest"  
          }  
        }  
      ]  
    }  
  ]  
}
```

```

    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 2,
    "OnDemandTargetCapacity": 0,
    "SpotTargetCapacity": 2,
    "DefaultTargetCapacityType": "spot"
  },
  "TerminateInstancesWithExpiration": false,
  "Type": "maintain",
  "ReplaceUnhealthyInstances": false,
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized",
    "InstanceInterruptionBehavior": "terminate"
  },
  "OnDemandOptions": {
    "AllocationStrategy": "lowestPrice"
  }
}
]
}

```

Utilisez la commande [describe-fleet-instances](#) suivante afin de décrire les instances pour le Flotte EC2 spécifié. La liste renvoyée des instances en cours d'exécution est actualisée périodiquement et peut ne pas être à jour.

```
aws ec2 describe-fleet-instances --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Exemple de sortie

```

{
  "ActiveInstances": [
    {
      "InstanceId": "i-09cd595998cb3765e",
      "InstanceHealth": "healthy",
      "InstanceType": "m4.large",
      "SpotInstanceRequestId": "sir-86k84j6p"
    },
    {
      "InstanceId": "i-09cf95167ca219f17",
      "InstanceHealth": "healthy",
      "InstanceType": "m4.large",

```

```

        "SpotInstanceRequestId": "sir-dvxi7fsm"
    }
],
"FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}

```

Utilisez la commande [describe-fleet-history](#) suivante afin de décrire l'historique du Flotte EC2 spécifié pour la période spécifiée.

```

aws ec2 describe-fleet-history --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE --
start-time 2018-04-10T00:00:00Z

```

Exemple de sortie

```

{
  "HistoryRecords": [
    {
      "EventInformation": {
        "EventSubType": "submitted"
      },
      "EventType": "fleetRequestChange",
      "Timestamp": "2020-09-01T18:26:05.000Z"
    },
    {
      "EventInformation": {
        "EventSubType": "active"
      },
      "EventType": "fleetRequestChange",
      "Timestamp": "2020-09-01T18:26:15.000Z"
    },
    {
      "EventInformation": {
        "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
        "EventSubType": "progress"
      },
      "EventType": "fleetRequestChange",
      "Timestamp": "2020-09-01T18:26:17.000Z"
    },
    {
      "EventInformation": {
        "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
        "EventSubType": "launched",
        "InstanceId": "i-083a1c446e66085d2"
      }
    }
  ]
}

```

```

    },
    "EventType": "instanceChange",
    "Timestamp": "2020-09-01T18:26:17.000Z"
  },
  {
    "EventInformation": {
      "EventDescription": "{\"instanceType\": \"t2.small\", ...}\",
      "EventSubType": "launched",
      "InstanceId": "i-090db02406cc3c2d6"
    },
    "EventType": "instanceChange",
    "Timestamp": "2020-09-01T18:26:17.000Z"
  }
],
"FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
"LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
"StartTime": "2018-04-09T23:53:20.000Z"
}

```

Modifier une flotte EC2

Vous pouvez modifier un Flotte EC2 qui présente l'état `submitted` ou `active`. Lorsque vous modifiez un parc d'instances, il prend l'état `modifying`.

Vous pouvez uniquement modifier un Flotte EC2 qui a le type `maintain`. Vous ne pouvez pas modifier un Flotte EC2 ayant le type `request` ou `instant`.

Vous pouvez modifier les paramètres suivants d'une flotte EC2 :

- `target-capacity-specification` – Augmentez ou diminuez la capacité cible pour `TotalTargetCapacity`, `OnDemandTargetCapacity` et `SpotTargetCapacity`.
- `excess-capacity-termination-policy` – Indiquez si les instances en cours d'exécution doivent être résiliées si la capacité cible totale du Flotte EC2 est définie sous la taille actuelle du parc d'instances. Les valeurs valides sont `no-termination` et `termination`.

Lorsque vous augmentez la capacité cible, la Flotte EC2 lance les instances supplémentaires en fonction de l'option d'achat d'instance spécifiée pour `DefaultTargetCapacityType`, qui correspond à des Instances à la demande ou à des Instances Spot.

Dans l'`DefaultTargetCapacityTypeaffirmativespot`, la flotte EC2 lance les instances ponctuelles supplémentaires conformément à sa [stratégie d'allocation](#).

Lorsque vous diminuez la capacité cible, la flotte EC2 supprime toutes les demandes ouvertes qui dépassent la nouvelle capacité cible. Vous pouvez demander à ce que la flotte d'instances mette hors service les instances jusqu'à ce que la taille de la flotte atteigne la nouvelle capacité cible. Si la stratégie d'allocation est `lowest-price`, le parc d'instances met hors service les instances ayant le prix par unité le plus élevé. En revanche, si la stratégie d'allocation est `diversified`, le parc d'instances met hors service les instances des divers pools. Vous pouvez aussi demander à ce que la flotte EC2 conserve sa taille actuelle, mais sans remplacer les instances Spot interrompues ni les instances que vous résiliez manuellement.

Lorsqu'une flotte EC2 résilie une instance Spot du fait de la diminution de la capacité cible, l'instance reçoit un avis d'interruption d'instance Spot.

Modifier une flotte EC2 (AWS CLI)

Utilisez la commande [modify-fleet](#) suivante pour mettre à jour la capacité cible de la Flotte EC2 spécifié.

```
aws ec2 modify-fleet \  
  --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \  
  --target-capacity-specification TotalTargetCapacity=20
```

Si vous diminuez la capacité cible, mais que vous souhaitez conserver la taille actuelle de la flotte, vous pouvez modifier la commande précédente comme suit :

```
aws ec2 modify-fleet \  
  --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \  
  --target-capacity-specification TotalTargetCapacity=10 \  
  --excess-capacity-termination-policy no-termination
```

Supprimer une flotte EC2

Si vous n'avez plus besoin d'une flotte EC2, vous pouvez le supprimer. Après la suppression d'une flotte, toutes les demandes Spot associées à la flotte sont annulées, de sorte qu'aucune nouvelle instance Spot n'est lancée.

Lorsque vous supprimez une flotte d'instances EC2, vous devez également spécifier si vous voulez résilier toutes ses instances. Cette action inclut les instances à la demande et les instances Spot. Pour les instant flottes, EC2 Fleet doit mettre fin aux instances lorsque la flotte est supprimée. Une flotte instant supprimé avec des instances en cours d'exécution n'est pas pris en charge.

Si vous spécifiez que les instances doivent être résiliées lors de la suppression de la flotte, celle-ci entre dans l'état `deleted_terminating`. Sinon, il passe à l'état `deleted_running` et les instances continuent à s'exécuter jusqu'à ce qu'elles soient interrompues ou jusqu'à ce que vous les mettiez hors service manuellement.

Restrictions

- Vous pouvez supprimer jusqu'à 25 flottes de types `instant` en une seule demande.
- Vous pouvez supprimer jusqu'à 100 flottes de types `maintain` ou `request` en une seule demande.
- Vous pouvez supprimer jusqu'à 125 flottes en une seule demande, à condition de ne pas dépasser le quota pour chaque type de flotte, comme indiqué ci-dessus.
- Si vous dépassez le nombre spécifié de flottes à supprimer, aucune flotte n'est supprimée.
- Jusqu'à 1 000 instances peuvent être résiliées en une seule demande de suppression de parcs `instant`.

Pour supprimer une flotte EC2 et résilier ses instances (AWS CLI)

Utilisez la commande [delete-fleets](#) et le paramètre `--terminate-instances` pour supprimer la flotte d'instances EC2 spécifiée et résilier les instances qui lui sont associées.

```
aws ec2 delete-fleets \  
  --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \  
  --terminate-instances
```

Exemple de sortie

```
{  
  "UnsuccessfulFleetDeletions": [],  
  "SuccessfulFleetDeletions": [  
    {  
      "CurrentFleetState": "deleted_terminating",  
      "PreviousFleetState": "active",  
      "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"  
    }  
  ]  
}
```

Pour supprimer une flotte d'instances EC2 sans résilier ses instances (AWS CLI)

Vous pouvez modifier la commande précédente avec le paramètre `--no-terminate-instances` pour supprimer la flotte d'instances EC2 spécifiée sans résilier les instances qui lui sont associées.

Note

`--no-terminate-instances` n'est pas pris en charge pour les parcs instant.

```
aws ec2 delete-fleets \  
  --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \  
  --no-terminate-instances
```

Exemple de sortie

```
{  
  "UnsuccessfulFleetDeletions": [],  
  "SuccessfulFleetDeletions": [  
    {  
      "CurrentFleetState": "deleted_running",  
      "PreviousFleetState": "active",  
      "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"  
    }  
  ]  
}
```

Dépannage lorsqu'une flotte ne peut pas être supprimé

Si un Flotte EC2 ne peut pas être supprimé, `UnsuccessfulFleetDeletions` dans la sortie renvoie l'ID du Flotte EC2, un code d'erreur et un message d'erreur.

Les codes d'erreur sont :

- `ExceededInstantFleetNumForDeletion`
- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`

- `unexpectedError`

Résolution des problèmes de `ExceededInstantFleetNumForDeletion`

Si vous essayez de supprimer plus de 25 parcs instant en une seule demande, l'erreur `ExceededInstantFleetNumForDeletion` est renvoyée. Voici un exemple de sortie pour cette erreur.

```
{
  "UnsuccessfulFleetDeletions": [
    {
      "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
      "Error": {
        "Message": "Can't delete more than 25 instant fleets in a single
request.",
        "Code": "ExceededInstantFleetNumForDeletion"
      }
    },
    {
      "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
      "Error": {
        "Message": "Can't delete more than 25 instant fleets in a single
request.",
        "Code": "ExceededInstantFleetNumForDeletion"
      }
    }
  ],
  "SuccessfulFleetDeletions": []
}
```

Résoudre les problèmes liés à `NoTerminateInstancesNotSupported`

Si vous spécifiez que les instances d'un parc instant ne doivent pas être résiliées lorsque vous supprimez le parc, l'erreur `NoTerminateInstancesNotSupported` est renvoyée. `--no-terminate-instances` n'est pas pris en charge pour les parcs instant. Voici un exemple de sortie pour cette erreur.

```
{
```

```

    "UnsuccessfulFleetDeletions": [
      {
        "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
        "Error": {
          "Message": "NoTerminateInstances option is not supported for
instant fleet",
          "Code": "NoTerminateInstancesNotSupported"
        }
      }
    ],
    "SuccessfulFleetDeletions": []
  }
}

```

Résoudre les problèmes liés à **UnauthorizedOperation**

Si vous n'avez pas l'autorisation de résilier des instances, vous obtenez l'erreur `UnauthorizedOperation` lors de la suppression d'un parc qui doit résilier ses instances. Voici le message d'erreur.

```

<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
authorized to perform this
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzyHasFH0aRYJpaDVravoW25azn6KNkUQQ1FwhJyujt2dtNCdduJfrqcFYAj1EiRMkfdHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNTqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdh10Ng6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtY0pYcE14_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1Px0DZuqWHs23YXWVyzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmK0_QIE8N8s6NWzCK4yoX-9gDcheur0GpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>

```

Pour résoudre l'erreur, vous devez ajouter l'action `ec2:TerminateInstances` à la stratégie IAM, comme illustré dans l'exemple suivant.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DeleteFleetsAndTerminateInstances",
      "Effect": "Allow",
      "Action": [

```

```
        "ec2:DeleteFleets"  
        "ec2:TerminateInstances"  
    ],  
    "Resource": "*" ]  
}
```

Parc d'instances Spot

Un parc d'instances Spot est un ensemble d'instances Spot et éventuellement d'instances à la demande qui est lancé en fonction des critères que vous avez spécifiés. Le parc d'instances Spot sélectionne les groupes de capacités Spot correspondants à vos besoins et lance les instances Spot de façon à répondre à la capacité cible de la flotte. Par défaut, un Parc d'instances Spot est configuré pour maintenir la capacité cible en lançant des instances de remplacement après la résiliation d'Instances Spot du parc. Vous pouvez envoyer un parc d'instances Spot comme une demande unique qui ne persiste pas après que les instances ont été résiliées. Vous pouvez inclure des demandes d'instance à la demande dans une demande de parc d'instances Spot .

Note

Si vous voulez utiliser une console pour créer une flotte qui inclut des instances Spot, nous vous recommandons d'utiliser un groupe Auto Scaling plutôt qu'un parc d'instances Spot. Pour plus d'informations, consultez [Groupes Auto Scaling avec types d'instance et options d'achat multiples](#) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

Si vous souhaitez utiliser le AWS CLI pour créer un parc incluant des instances Spot, nous vous recommandons d'utiliser un groupe Auto Scaling ou un parc EC2 plutôt qu'un parc Spot. L'API [RequestSpotFleet](#), sur laquelle Spot Fleet est basé, est une ancienne API sans investissement prévu.

Pour plus d'informations sur les API qu'il est recommandé d'utiliser, consultez [Quelle est la meilleure méthode de demande Spot à utiliser ?](#)

Rubriques

- [Types de demande de parc d'instances Spot](#)
- [Stratégies de configuration d'un parc d'instances Spot](#)
- [Utilisation de flottes d'instances Spot](#)
- [CloudWatch métriques pour Spot Fleet](#)
- [Scalabilité automatique du parc d'instances Spot](#)

Types de demande de parc d'instances Spot

Il existe deux types de demandes de parc d'instances Spot :

request

Si vous configurez le type de demande comme `request`, le parc d'instances Spot passe une demande unique asynchrone de la capacité souhaitée. Ensuite, si la capacité est réduite en raison d'interruptions Spot, la flotte d'instances n'essaie pas de réapprovisionner les instances Spot et il ne soumet pas les demandes dans d'autres groupes de capacité Spot si la capacité n'est pas disponible.

maintain

Si vous configurez le type de demande comme `maintain`, le parc d'instances Spot passe une demande asynchrone de la capacité souhaitée et maintient la capacité en réapprovisionnant automatiquement les instances Spot interrompues.

Pour spécifier le type de demande dans la console Amazon EC2, procédez comme suit lors de la création d'une demande de parc d'instances Spot :

- Pour créer un parc d'instances Spot de type `request`, effacez la case `Maintain target capacity` (Maintenir la capacité cible).
- Pour créer un parc d'instances Spot de type `maintain`, choisissez la case `Maintain target capacity` (Maintenir la capacité cible).

Pour plus d'informations, consultez [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#).

Les deux types de demande bénéficient d'une stratégie d'allocation. Pour plus d'informations, consultez [Stratégies d'allocation pour instances Spot](#).

Stratégies de configuration d'un parc d'instances Spot

Un parc d'instances Spot est un ensemble, ou une flotte, d'instances Spot et, facultativement, d'instances à la demande.

Le parc d'instances Spot tente de lancer le nombre d'instances Spot et d'instances à la demande afin de répondre à la capacité cible que vous avez spécifiée dans la demande de parc d'instances Spot. La demande des instances Spot est satisfaite si le prix maximal que vous avez spécifié dans la demande dépasse le prix spot actuel et si la capacité est disponible. Le parc d'instances Spot tente également de préserver sa flotte de capacité cible si les instances Spot sont interrompues.

Vous pouvez également définir le montant maximum que vous êtes prêt à payer par heure pour votre flotte et le parc d'instances Spot lance les instances jusqu'à ce que le montant maximum soit atteint. Une fois le montant maximum que vous être prêt à payer atteint, la flotte arrête de lancer des instances même si la capacité cible n'a pas été atteinte.

Un groupe de capacités Spot est un ensemble d'instances EC2 inutilisées ayant les mêmes type d'instance (par exemple `m5.large`), système d'exploitation, zone de disponibilité et plateforme réseau. Lorsque vous effectuez une demande de parc d'instances Spot, vous pouvez inclure plusieurs spécifications de lancement qui varient selon le type d'instance, l'AMI, la zone de disponibilité ou le sous-réseau. Le parc d'instances Spot sélectionne les groupes de capacités Spot servant à satisfaire la demande, selon les spécifications de lancement incluses dans votre demande de parc d'instances Spot et la configuration de cette demande. Les instances Spot proviennent des groupes sélectionnés.

Table des matières

- [Planification d'une demande de parc d'instances Spot](#)
- [Stratégies d'allocation pour instances Spot](#)
- [Sélection de type d'instance basée sur des attributs pour un parc d'instances Spot](#)
- [À la demande dans la demande de parc d'instances Spot](#)
- [Rééquilibrage de la capacité](#)
- [Remplacements du prix Spot](#)
- [Contrôle des dépenses](#)
- [Pondération d'instance de parc d'instances Spot](#)

Planification d'une demande de parc d'instances Spot

Avant de créer une demande de parc d'instances Spot, passez en revue les [bonnes pratiques en matière d'instances Spot](#). Appuyez-vous sur ces bonnes pratiques lorsque vous planifiez votre demande de parc d'instances Spot de façon à allouer le type d'instance souhaité au prix le plus bas possible. Nous vous recommandons également d'effectuer les opérations suivantes :

- Déterminez si vous souhaitez créer un parc d'instances Spot qui envoie une demande unique pour la capacité cible souhaitée ou qui doit maintenir une capacité cible dans le temps.
- Déterminez les types d'instance qui correspondent aux exigences de votre application.

- Déterminez la capacité cible de votre demande de parc d'instances Spot . Vous pouvez définir la capacité cible en instances ou en unités personnalisées. Pour plus d'informations, consultez [Pondération d'instance de parc d'instances Spot](#) .
- Déterminez quelle portion de la capacité cible du parc d'instances Spot doit correspondre à la capacité à la demande. Vous pouvez spécifier une capacité à la demande égale à 0.
- Déterminez le prix par unité si vous avez recours à la pondération d'instance. Pour calculer le prix par unité, divisez le prix pour une heure d'instance par le nombre d'unités (ou pondération) que cette instance représente. Si vous n'utilisez pas la pondération d'instance, le prix par unité défini par défaut est le prix par heure d'instance.
- Passez en revue les options possibles pour votre demande de parc d'instances Spot . Pour plus d'informations, consultez la section sur la commande [request-spot-fleet](#) dans le document AWS CLI Référence des commandes. Pour accéder à des exemples supplémentaires, consultez [Exemples de configuration d'un parc d'instances Spot](#).

Stratégies d'allocation pour instances Spot

Votre configuration du lancement détermine tous les groupes de capacité Spot possibles (types d'instance et zones de disponibilité) à partir desquels le parc d'instances Spot peut lancer des instances Spot. Cependant, lors du lancement des instances, le parc d'instances Spot utilise la stratégie d'allocation que vous spécifiez pour choisir les groupes spécifiques parmi tous vos groupes possibles.

Note

(Instances Linux uniquement) Si vous configurez votre instance Spot pour qu'elle soit lancée alors qu'[AMD SEV-SNP](#) est activé, des frais d'utilisation horaires supplémentaires équivalant à 10 % du [taux horaire à la demande pour le type](#) d'instance sélectionné vous sont facturés. Si la stratégie d'allocation utilise le prix comme entrée, la flotte EC2 n'inclut pas ces frais supplémentaires ; seul le prix Spot est utilisé.

Stratégies d'allocation

Vous pouvez spécifier l'une des stratégies d'allocation suivantes pour vos instances Spot :

`priceCapacityOptimized`(recommandé)

Le parc d'instances Spot identifie les groupes dotés des capacités disponibles les plus élevées pour le nombre d'instances qui sont lancées. Cela signifie que nous demanderons des instances Spot auprès des groupes qui, selon nous, présentent le moins de risques d'interruption à court terme. Le parc d'instances Spot demande ensuite des instances Spot auprès du pool le moins coûteux de ces pools.

La stratégie d'allocation `priceCapacityOptimized` constitue le meilleur choix pour la plupart des charges de travail Spot, telles que les applications conteneurisées sans état, les microservices, les applications Web, les tâches de données et d'analyse, ainsi que le traitement par lots.

`capacityOptimized`

Le parc d'instances Spot identifie les groupes dotés des capacités disponibles les plus élevées pour le nombre d'instances qui sont lancées. Cela signifie que nous demanderons des instances Spot auprès des groupes qui, selon nous, présentent le moins de risques d'interruption à court terme. Vous pouvez éventuellement définir une priorité pour chaque type d'instance de votre parc à l'aide de la commande `capacityOptimizedPrioritized`. Le parc d'instances Spot optimise la capacité d'abord, mais respecte les priorités de type d'instance sur la base du meilleur effort.

Avec les instances Spot, la tarification change lentement au fil du temps en fonction des tendances à long terme en matière d'offre et de demande, mais la capacité fluctue en temps réel. La stratégie `capacityOptimized` lance automatiquement des Instances Spot dans les pools les plus disponibles en examinant les données de capacité en temps réel et en prédisant les instances les plus disponibles. Cela convient parfaitement aux charges de travail dont l'interruption entraîne des coûts plus élevés associés au travail de redémarrage, telles que le temps d'intégration continue (CI), le rendu d'images et de médias, le deep learning, ainsi que les charges de travail de calcul haute performance (HPC), qui peuvent avoir un coût d'interruption plus élevé associées au travail de redémarrage. En offrant la possibilité de moins d'interruptions, la stratégie `capacityOptimized` peut réduire le coût global de votre charge de travail.

Alternativement, vous pouvez utiliser la stratégie d'allocation `capacityOptimizedPrioritized` avec un paramètre de priorité pour définir l'ordre des types d'instance à utiliser de la priorité la plus élevée à la plus basse. Vous pouvez définir la même priorité pour différents types d'instance. Le parc d'instances Spot optimisera d'abord la capacité, mais respectera les priorités de type d'instance sur la base du meilleur effort (par exemple, si le respect des priorités n'affecte pas de manière significative la capacité du parc d'instances Spot à fournir une capacité optimale). C'est une bonne option pour les charges de travail pour

lesquelles la possibilité de perturbation doit être minimisée, mais la priorité de certains types d'instances est également importante. L'utilisation des priorités n'est prise en charge que si votre flotte utilise un modèle de lancement. Notez que lorsque vous définissez la priorité sur `capacityOptimizedPrioritized`, la même priorité est également appliquée à vos instances à la demande si l'option à la demande `AllocationStrategy` est définie sur `prioritized`.

`diversified`

Les instances Spot sont réparties entre tous les groupes.

Choisir une stratégie d'allocation appropriée

Vous pouvez optimiser votre flotte en fonction de votre cas d'utilisation en choisissant la stratégie d'allocation de points appropriée. Pour ce qui est de la capacité cible des instances à la demande, Spot Fleet sélectionne toujours le type d'instance le moins cher en fonction du prix public à la demande, tout en suivant la stratégie d'allocation (soit `priceCapacityOptimizedcapacityOptimized`, soit) pour les instances ponctuelles `diversified`.

Trouver un équilibre entre le prix le plus bas et la capacité disponible

Pour trouver un équilibre entre les groupes de capacité Spot les moins chers et les groupes de capacité Spot présentant la disponibilité de capacité la plus élevée, nous vous recommandons d'utiliser la stratégie d'allocation `priceCapacityOptimized`. Cette stratégie prend des décisions concernant les groupes auprès desquels il convient de demander des instances Spot en fonction à la fois du prix des groupes et de la capacité disponible des instances Spot dans ces groupes. Cela signifie que nous demanderons des instances Spot auprès des groupes qui, selon nous, présentent le moins de risques d'interruption à court terme, tout en tenant compte du prix.

Si votre flotte exécute des charges de travail résilientes et sans état, notamment des applications conteneurisées, des microservices, des applications web, des tâches de données et d'analyse et des traitements par lots, utilisez la stratégie d'allocation `priceCapacityOptimized` pour optimiser les économies de coûts et la capacité disponible.

Si votre flotte exécute des charges de travail dont l'interruption entraîne des coûts plus élevés associés au travail de redémarrage, vous devez implémenter des points de contrôle afin que les applications puissent redémarrer à partir de ce point, si elles sont interrompues. En utilisant des points de contrôle, vous adaptez la stratégie d'allocation `priceCapacityOptimized` à ces charges de travail, car elle alloue la capacité à partir des groupes les moins chers qui offrent également un faible taux d'interruption des instances Spot.

Pour un exemple de configuration utilisant la stratégie d'allocation `priceCapacityOptimized`, reportez-vous à la section [Exemple 9 : Lancer des instances ponctuelles dans un parc à capacité optimisée avec des priorités](#).

Lorsque les charges de travail ont un coût d'interruption élevé

Vous pouvez éventuellement utiliser la stratégie `capacityOptimized` si vous exécutez des charges de travail utilisant des types d'instances dont le prix est similaire, ou lorsque le coût des interruptions est si important que toute économie de coûts est insuffisante par rapport à une augmentation marginale du nombre d'interruptions. Cette stratégie alloue la capacité à partir des groupes de capacité Spot les plus disponibles qui offrent la possibilité de moins d'interruptions, ce qui peut réduire le coût global de votre charge de travail. Pour un exemple de configuration utilisant la stratégie d'allocation `capacityOptimized`, reportez-vous à la section [Exemple 7 : configurer le rééquilibrage de capacité pour lancer des instances Spot de remplacement](#).

Lorsque le risque d'interruption doit être minimisé, mais que la préférence pour certains types d'instance est importante, vous pouvez exprimer vos priorités de groupe en utilisant la stratégie d'allocation `capacityOptimizedPrioritized`, puis définir l'ordre des types d'instance à utiliser de la priorité la plus élevée à la plus basse. Pour accéder à un exemple de configuration, consultez [Exemple 8 : Lancer des instances ponctuelles dans un parc à capacité optimisée](#).

Veillez noter que l'utilisation des priorités n'est prise en charge que si votre flotte utilise un modèle de lancement. Notez aussi que lorsque vous définissez les priorités sur `capacityOptimizedPrioritized`, les mêmes priorités sont également appliquées à vos instances à la demande si l'option à la demande `AllocationStrategy` est définie sur `prioritized`.

Lorsque votre charge de travail est flexible dans le temps et que la capacité disponible n'est pas un facteur

Si votre flotte est de petite taille ou si elle s'exécute pendant un temps limité, vous pouvez utiliser `priceCapacityOptimized` pour maximiser vos économies tout en tenant compte de la capacité disponible.

Lorsque votre flotte est importante ou s'exécute pendant une longue période

Si votre parc est important ou qu'il s'exécute pendant une longue durée, vous pouvez améliorer sa disponibilité en répartissant les Instances Spot entre plusieurs groupes en utilisant la stratégie `diversified`. Par exemple, si votre parc d'instances Spot spécifie 10 groupes et une capacité cible

de 100 instances, la flotte lance 10 instances Spot dans chaque groupe. Si le prix Spot d'un pool dépasse le prix maximum de ce pool, seul 10 % de votre flotte est touché. Avec cette stratégie, votre flotte est également moins affecté par les augmentations du prix Spot dans un pool au fil du temps. Avec la stratégie `diversified`, le parc d'instances Spot ne lance pas d'instances Spot dans des groupes dont le prix Spot est supérieur ou égal au [prix à la demande](#).

Maintenir la capacité cible

Une fois les instances Spot résiliées en raison d'un changement de prix Spot ou de la modification de la capacité disponible d'un groupe de capacités Spot, un parc d'instances Spot de type `maintain` lance des instances Spot de remplacement. La stratégie d'allocation détermine les groupes à partir desquels les instances de remplacement sont lancées, comme suit :

- Si la stratégie d'allocation est `priceCapacityOptimized`, la flotte lance les instances de remplacement dans les groupes présentant le plus de capacités d'instances Spot disponibles, tout en tenant compte du prix et en identifiant les groupes les moins chers avec une capacité disponible élevée.
- Si la stratégie d'allocation `capacityOptimized` est sélectionnée, la flotte lance les instances de remplacement dans les groupes avec le plus de capacités d'instances Spot disponibles.
- Si la stratégie d'allocation est `diversified`, le parc d'instances répartit les Instances Spot de remplacement entre les groupes restants.

Sélection de type d'instance basée sur des attributs pour un parc d'instances Spot

Lorsque vous créez un parc d'instances Spot, vous devez spécifier un ou plusieurs types d'instance pour configurer les instances à la demande et les instances Spot de la flotte. Au lieu de spécifier manuellement les types d'instance, vous pouvez spécifier les attributs qu'une instance doit posséder, et Amazon EC2 identifiera tous les types d'instance avec ces attributs. C'est ce qu'on appelle la sélection de type d'instance basée sur des attributs. Par exemple, vous pouvez spécifier le nombre minimal et maximal de vCPU requis pour vos instances, et le parc d'instances Spot lancera les instances à l'aide de tous les types d'instance disponibles répondant à ces exigences de vCPU.

La sélection de type d'instance basée sur des attributs est idéale pour les charges de travail et les cadres qui peuvent être flexibles quant aux types d'instances qu'ils utilisent, par exemple lors de l'exécution de conteneurs ou de flottes web, du traitement de big data et de la mise en œuvre d'outils de CI/CD (intégration et déploiement continu).

Avantages

La sélection de type d'instance basée sur des attributs présente les avantages suivants :

- Utilisez facilement les bons types d'instances : compte tenu du grand nombre de types d'instances disponibles, la recherche des types d'instances adaptés à votre charge de travail peut prendre beaucoup de temps. Lorsque vous spécifiez des attributs d'instance, les types d'instance auront automatiquement les attributs requis pour votre charge de travail.
- Configuration simplifiée — Pour spécifier manuellement plusieurs types d'instances pour un parc de spots, vous devez créer un modèle de lancement distinct pour chaque type d'instance. Toutefois, avec la sélection de type d'instance basée sur des attributs, pour fournir plusieurs types d'instance, il suffit de spécifier les attributs d'instance dans le modèle de lancement ou dans un remplacement de modèle de lancement.
- Utilisation automatique de nouveaux types d'instances : lorsque vous spécifiez des attributs d'instance plutôt que des types d'instances, votre parc peut utiliser des types d'instances de nouvelle génération au fur et à mesure de leur publication, afin de « pérenniser » la configuration du parc.
- Flexibilité des types d'instances — Lorsque vous spécifiez des attributs d'instance plutôt que des types d'instances, Spot Fleet peut choisir parmi un large éventail de types d'instances pour lancer des instances Spot, conformément aux [meilleures pratiques Spot en matière de flexibilité des types d'instances](#).

Rubriques

- [Fonctionnement de la sélection de type d'instance basée sur des attributs](#)
- [Protection des prix](#)
- [Considérations](#)
- [Créer un parc d'instances Spot avec une sélection de type d'instance basée sur des attributs](#)
- [Exemples de configurations valides et non valides](#)
- [Aperçu des types d'instances avec des attributs spécifiés](#)

Fonctionnement de la sélection de type d'instance basée sur des attributs

Pour utiliser la sélection de type d'instance basée sur des attributs dans la configuration de votre flotte, vous remplacez la liste des types d'instance par une liste d'attributs d'instance dont vos instances ont besoin. Le parc d'instances Spot lance des instances sur tous les types d'instance disponibles possédant les attributs d'instance spécifiés.

Rubriques

- [Types d'attributs d'instance](#)
- [Où configurer la sélection de type d'instance basée sur des attributs](#)
- [Comment le parc d'instances Spot utilise la sélection de type d'instance basée sur des attributs lors de l'approvisionnement d'une flotte](#)

Types d'attributs d'instance

Il existe plusieurs attributs d'instance que vous pouvez spécifier pour exprimer vos besoins en matière de calcul, tels que :

- Nombre de vCPU : nombre minimum et maximum de vCPU par instance.
- Mémoire : mémoire minimale et maximale GiBs par instance.
- Stockage local : s'il faut utiliser EBS ou des volumes de stockage d'instance pour le stockage local.
- Performances éclatantes : s'il faut utiliser la famille d'instances T, y compris les types T4g, T3a, T3 et T2.

Pour une description de chaque attribut et des valeurs par défaut, consultez le [InstanceRequirements](#) manuel Amazon EC2 API Reference.

Où configurer la sélection de type d'instance basée sur des attributs

Selon que vous utilisez la console ou le AWS CLI, vous pouvez spécifier les attributs d'instance pour la sélection du type d'instance basée sur les attributs comme suit :

Dans la console, vous pouvez spécifier les attributs d'instance dans l'un des composants ou les deux composants de configuration de flotte suivants :

- Dans un modèle de lancement, puis référencez le modèle de lancement dans la demande de flotte
- Dans la demande de flotte

Dans le AWS CLI, vous pouvez spécifier les attributs d'instance dans l'un ou l'ensemble des composants de configuration de flotte suivants :

- Dans un modèle de lancement, et référencez le modèle de lancement dans la demande de flotte
- Dans un remplacement de modèle de lancement

Si vous souhaitez combiner des instances utilisant différentes AMI, vous pouvez spécifier des attributs d'instance dans plusieurs remplacements de modèles de lancement. Par exemple, différents types d'instance peuvent utiliser des processeurs x86 et Arm.

- Dans une spécification de lancement

Comment le parc d'instances Spot utilise la sélection de type d'instance basée sur des attributs lors de l'approvisionnement d'une flotte

Le parc d'instances Spot alloue une flotte de la manière suivante :

- Le parc d'instances Spot identifie les types d'instance qui possèdent les attributs spécifiés.
- Le parc d'instances Spot utilise la protection des prix pour déterminer les types d'instance à exclure.
- Spot Fleet détermine les pools de capacités à partir desquels il envisagera de lancer les instances en fonction des AWS régions ou des zones de disponibilité présentant les types d'instances correspondants.
- Le parc d'instances Spot applique la stratégie d'allocation spécifiée pour déterminer les groupes de capacités à partir desquels lancer les instances.

Notez que la sélection de type d'instance basée sur des attributs ne permet pas de sélectionner les groupes de capacités à partir desquels allouer la flotte ; c'est la tâche des stratégies d'allocation. Il peut y avoir un grand nombre de types d'instances avec des attributs spécifiés, et certains d'entre eux peuvent être coûteux.

Si vous spécifiez une stratégie d'allocation, le parc d'instances Spot lance des instances conformément à la stratégie d'allocation spécifiée.

- Pour les instances Spot, la sélection de type d'instance basée sur des attributs prend en charge les stratégies d'allocation `capacityOptimizedPrioritized` et `capacityOptimized`.
- Pour les instances à la demande, la sélection du type d'instance basée sur les attributs soutient la stratégie `lowestPrice` d'allocation, qui garantit que Spot Fleet lancera des instances à la demande à partir des pools de capacités les moins coûteux.
- S'il n'y a pas de capacité pour les types d'instance avec des attributs d'instance spécifiés, aucune instance ne peut être lancée et la flotte renvoie une erreur.

Protection des prix

La protection des prix est une fonction qui empêche votre parc d'instances Spot d'utiliser des types d'instance que vous considéreriez trop chers même s'ils correspondent aux attributs que vous avez spécifiés. Pour utiliser la protection des prix, vous devez définir un seuil de prix. Ensuite, lorsqu'Amazon EC2 sélectionne des types d'instances avec vos attributs, il exclut les types d'instances dont le prix est supérieur à votre seuil.

Amazon EC2 calcule le seuil de prix de la manière suivante :

- Amazon EC2 identifie d'abord le type d'instance le moins cher parmi ceux qui correspondent à vos attributs.
- Amazon EC2 prend ensuite la valeur (exprimée en pourcentage) que vous avez spécifiée pour le paramètre de protection des prix et la multiplie par le prix du type d'instance identifié. Le résultat est le prix qui est utilisé comme seuil de prix.

Il existe des seuils de prix distincts pour les instances à la demande et les instances ponctuelles.

Lorsque vous créez un parc avec sélection du type d'instance basée sur les attributs, la protection des prix est activée par défaut. Vous pouvez conserver les valeurs par défaut ou définir les vôtres.

Vous pouvez également désactiver la protection des prix. Pour n'indiquer aucun seuil de protection des prix, spécifiez une valeur en pourcentage élevée, telle que 999999.

Rubriques

- [Comment est identifié le type d'instance le moins cher](#)
- [Protection du prix des instances à la demande](#)
- [Protection des prix des instances Spot](#)
- [Spécifiez le seuil de protection des prix](#)

Comment est identifié le type d'instance le moins cher

Amazon EC2 détermine le prix sur lequel baser le seuil de prix en identifiant le type d'instance dont le prix est le plus bas parmi celles qui correspondent aux attributs que vous avez spécifiés. Pour ce faire, il procède de la manière suivante :

- Il examine d'abord les types d'instances C, M ou R de la génération actuelle qui correspondent à vos attributs. S'il trouve des correspondances, il identifie le type d'instance le moins cher.

- S'il n'y a pas de correspondance, il examine ensuite tous les types d'instances de la génération actuelle qui correspondent à vos attributs. S'il trouve des correspondances, il identifie le type d'instance le moins cher.
- S'il n'y a pas de correspondance, il examine ensuite tous les types d'instances de la génération précédente qui correspondent à vos attributs et identifie le type d'instance le moins cher.

Protection du prix des instances à la demande

Le seuil de protection des prix pour les types d'instances à la demande est calculé sous la forme d'un pourcentage supérieur au type d'instance à la demande le moins cher identifié (`OnDemandMaxPricePercentageOverLowestPrice`). Vous spécifiez le pourcentage supérieur que vous êtes prêt à payer. Si vous ne spécifiez pas ce paramètre, la valeur par défaut de 20 est utilisée pour calculer un seuil de protection des prix supérieur de 20 % au prix identifié.

Par exemple, si le prix de l'instance On-Demand identifié est 0.4271, et que vous le spécifiez 25, le seuil de prix est supérieur de 25 % à 0.4271. Il est calculé comme suit : $0.4271 * 1.25 = 0.533875$. Le prix calculé est le montant maximum que vous êtes prêt à payer pour les instances à la demande et, dans cet exemple, Amazon EC2 exclura tous les types d'instances à la demande dont le coût est supérieur à 0.533875.

Protection des prix des instances Spot

Par défaut, Amazon EC2 applique automatiquement une protection optimale du prix des instances Spot afin de sélectionner de manière cohérente un large éventail de types d'instances. Vous pouvez également définir vous-même la protection des prix manuellement. Toutefois, laisser Amazon EC2 le faire à votre place peut améliorer les chances que votre capacité Spot soit atteinte.

Vous pouvez définir manuellement la protection des prix à l'aide de l'une des options suivantes. Si vous définissez manuellement la protection des prix, nous vous recommandons d'utiliser la première option.

- Pourcentage du type d'instance à la demande le moins cher identifié
[`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

Par exemple, si le prix du type d'instance On-Demand identifié est 0.4271, et que vous le spécifiez 60, le seuil de prix est de 60 % 0.4271. Il est calculé comme suit : $0.4271 * 0.60 = 0.25626$. Le prix calculé est le montant maximum que vous êtes prêt à payer pour les instances Spot et, dans cet exemple, Amazon EC2 exclura tous les types d'instances Spot dont le coût est supérieur à 0.25626.

- Un pourcentage supérieur au type d'instance Spot le moins cher identifié
[SpotMaxPricePercentageOverLowestPrice]

Par exemple, si le prix du type d'instance Spot identifié est 0.1808, et que vous le spécifiez 25, le seuil de prix est supérieur de 25 % à 0.1808. Il est calculé comme suit : $0.1808 * 1.25 = 0.226$. Le prix calculé est le montant maximum que vous êtes prêt à payer pour les instances Spot et, dans cet exemple, Amazon EC2 exclura tous les types d'instances Spot dont le coût est supérieur à 0.266. Nous vous déconseillons d'utiliser ce paramètre car les prix au comptant peuvent fluctuer et, par conséquent, votre seuil de protection contre les prix peut également fluctuer.

Spécifiez le seuil de protection des prix

Pour spécifier le seuil de protection des prix

Lors de la création du parc d'instances Spot, configurez la flotte pour la sélection du type d'instance basée sur des attributs, puis procédez comme suit :

- Console

Pour spécifier le seuil de protection des prix des instances à la demande, sous Additional instance attribute (Attribut d'instance supplémentaire), choisissez On-demand price protection (Protection des prix à la demande), puis Add attribute (Ajouter un attribut). Pour On-Demand price protection percentage (Pourcentage de protection des prix à la demande), saisissez le seuil de protection des prix sous forme de pourcentage.

Pour spécifier le seuil de protection des prix des instances Spot, sous Additional instance attribute (Attribut d'instance supplémentaire), choisissez Spot price protection (Protection des prix Spot), puis Add attribute (Ajouter un attribut). Choisissez un paramètre et entrez le seuil de protection des prix sous forme de pourcentage.

- AWS CLI

Pour spécifier le seuil de protection des prix de l'instance à la demande, dans le fichier de configuration JSON, dans la structure InstanceRequirements, pour OnDemandMaxPricePercentageOverLowestPrice, saisissez le seuil de protection des prix sous forme de pourcentage.

Pour spécifier le seuil de protection des prix des instances Spot, dans le fichier de configuration JSON, dans la InstanceRequirements structure, spécifiez l'un des paramètres suivants :

- Pour `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`, entrez le seuil de protection des prix sous forme de pourcentage.
- Pour `SpotMaxPricePercentageOverLowestPrice`, entrez le seuil de protection des prix sous forme de pourcentage.

Pour plus d'informations sur la création de flottes, veuillez consulter [Créer un parc d'instances Spot avec une sélection de type d'instance basée sur des attributs](#).

Note

Lors de la création du parc d'instances Spot, si vous définissez le type de `Total target capacity` (Capacité cible totale) sur `vCPUs` ou `Memory (MiB)` (Mémoire (MiB)) (console) ou `TargetCapacityUnitType` sur `vcpu` ou `memory-mib` (AWS CLI), le seuil de protection des prix s'applique en fonction du prix par vCPU ou par mémoire au lieu du prix par instance.

Considérations

- Vous pouvez spécifier des types d'instance ou des attributs d'instance dans un parc d'instances Spot, mais pas les deux en même temps.

Lorsque vous utilisez la CLI, les remplacements du modèle de lancement remplacent le modèle de lancement. Par exemple, si le modèle de lancement contient un type d'instance et que le remplacement du modèle de lancement contient des attributs d'instance, les instances identifiées par les attributs d'instance remplaceront le type d'instance dans le modèle de lancement.

- Lorsque vous utilisez la CLI, si vous spécifiez des attributs d'instance comme remplacements, vous ne pouvez pas non plus spécifier de pondérations ou de priorités.
- Vous pouvez spécifier un maximum de quatre structures `InstanceRequirements` dans une configuration de demande.

Créer un parc d'instances Spot avec une sélection de type d'instance basée sur des attributs

Vous pouvez configurer une flotte pour qu'elle utilise la sélection de type d'instance basée sur des attributs à l'aide de la console Amazon EC2 ou de la AWS CLI.

Rubriques

- [Créer un parc d'instances Spot à l'aide de la console](#)

- [Créez une flotte de spots à l'aide du AWS CLI](#)

Créer un parc d'instances Spot à l'aide de la console

Pour configurer un parc d'instances Spot pour la sélection de type d'instance basée sur des attributs (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Spot Requests (Demandes Spot) et sélectionnez Request Spot Instances (Demander des instances Spot).
3. Suivez les étapes permettant de créer un parc d'instances Spot. Pour plus d'informations, consultez [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#).

Lors de la création du parc d'instances Spot, configurez la flotte pour la sélection du type d'instance basée sur des attributs comme suit :

- a. Pour Instance type requirements (Exigences de type d'instance), choisissez Specify instance attributes that match your compute requirements (Spécifiez les attributs d'instance qui correspondent à vos exigences de calcul).
- b. Pour vCPU, saisissez les nombres minimum et maximum de vCPU souhaités. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.
- c. Pour Memory (GiB) (Mémoire (Gio)), saisissez la quantité minimale et maximale de mémoire souhaitée. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.
- d. (Facultatif) Pour Additional instance attributes (Attributs d'instance supplémentaires), vous pouvez éventuellement spécifier un ou plusieurs attributs pour exprimer vos exigences de calcul plus en détail. Chaque attribut supplémentaire ajoute des contraintes supplémentaires à votre demande.
- e. (Facultatif) Pour afficher les types d'instance avec vos attributs spécifiés, développez Preview matching instance types (Aperçu des types d'instance correspondants).

Créez une flotte de spots à l'aide du AWS CLI

Pour configurer un parc d'instances Spot pour la sélection de type d'instance basée sur des attributs (AWS CLI)

Utilisez la commande [request-spot-fleet](#) (AWS CLI) pour créer un parc d'instances Spot. Spécifiez la configuration de flotte dans un fichier JSON.

```
aws ec2 request-spot-fleet \  
  --region us-east-1 \  
  --spot-fleet-request-config file://file_name.json
```

Exemple de fichier *file_name*.json

L'exemple suivant contient les paramètres qui configurent un parc d'instances Spot afin qu'il utilise la sélection de type d'instance basée sur des attributs et est suivi d'une explication textuelle.

```
{  
  "AllocationStrategy": "priceCapacityOptimized",  
  "TargetCapacity": 20,  
  "Type": "request",  
  "LaunchTemplateConfigs": [{  
    "LaunchTemplateSpecification": {  
      "LaunchTemplateName": "my-launch-template",  
      "Version": "1"  
    },  
    "Overrides": [{  
      "InstanceRequirements": {  
        "VCpuCount": {  
          "Min": 2  
        },  
        "MemoryMiB": {  
          "Min": 4  
        }  
      }  
    }  
  ]  
}]  
}
```

Les attributs de sélection du type d'instance basé sur des attributs sont spécifiés dans la structure InstanceRequirements. Dans cet exemple, deux attributs sont spécifiés :

- `VCpuCount` : au moins 2 vCPU sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.
- `MemoryMiB` : au moins 4 Mio de mémoire sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.

Tout type d'instance doté d'au moins 2 vCPU et d'au moins 4 Mio de mémoire sera identifié.

Toutefois, la protection des prix et la stratégie d'allocation peuvent exclure certains types d'instances lorsque [le parc d'instances Spot alloue la flotte](#).

Pour obtenir une liste et une description de tous les attributs possibles que vous pouvez spécifier, consultez le [InstanceRequirements](#) manuel Amazon EC2 API Reference.

Note

Lorsque `InstanceRequirements` est inclus dans la configuration de la flotte, `InstanceType` et `WeightedCapacity` doivent être exclus. Ils ne peuvent pas déterminer la configuration de la flotte en même temps que les attributs d'instance.

Le JSON contient également la configuration de flotte suivante :

- `"AllocationStrategy"`: `"priceCapacityOptimized"` : la stratégie d'allocation des instances Spot de la flotte.
- `"LaunchTemplateName"`: `"my-launch-template"`, `"Version"`: `"1"` : le modèle de lancement contient certaines informations de configuration d'instance, mais si des types d'instance sont spécifiés, ils seront remplacés par les attributs spécifiés dans `InstanceRequirements`.
- `"TargetCapacity"`: `20` : la capacité cible est de 20 instances Spot.
- `"Type"`: `"request"` : le type de demande pour la flotte est `request`.

Exemples de configurations valides et non valides

Si vous utilisez le AWS CLI pour créer une flotte ponctuelle, vous devez vous assurer que la configuration de votre flotte est valide. Les exemples suivants illustrent les configurations valides et non valides.

Les configurations sont considérées comme non valides lorsqu'elles contiennent les éléments suivants :

- Une seule structure `Overrides` avec `InstanceRequirements` et `InstanceType`
- Deux structures `Overrides`, l'une avec `InstanceRequirements` et l'autre avec `InstanceType`
- Deux structures `InstanceRequirements` avec des valeurs d'attributs qui se chevauchent au sein du même `LaunchTemplateSpecification`

Exemples de configuration

- [Configuration valide : modèle de lancement unique avec remplacements](#)
- [Configuration valide : modèle de lancement unique avec plusieurs `InstanceRequirements`](#)
- [Configuration valide : deux modèles de lancement, chacun avec des remplacements](#)
- [Configuration valide : uniquement `InstanceRequirements` est spécifié, les valeurs d'attribut ne se chevauchent pas](#)
- [Configuration non valide : les `Overrides` contiennent `InstanceRequirements` et `InstanceType`](#)
- [Configuration non valide : deux `Overrides` contiennent `InstanceRequirements` et `InstanceType`](#)
- [Configuration non valide : chevauchement des valeurs d'attribut](#)

Configuration valide : modèle de lancement unique avec remplacements

La configuration suivante est valide. Elle contient un modèle de lancement et une structure `Overrides` contenant une structure `InstanceRequirements`. Vous trouverez ci-dessous une explication textuelle de l'exemple de configuration.

```
{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchTemplateConfigs": [
      {
        "LaunchTemplateSpecification": {
          "LaunchTemplateName": "My-launch-template",
          "Version": "1"
        },
        "Overrides": [
          {
            "InstanceRequirements": {
              "VCpuCount": {
```

```

        "Min": 2,
        "Max": 8
    },
    "MemoryMib": {
        "Min": 0,
        "Max": 10240
    },
    "MemoryGiBPerVCpu": {
        "Max": 10000
    },
    "RequireHibernateSupport": true
}
    ]
}
],
    "TargetCapacity": 5000,
    "OnDemandTargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu"
}
}

```

InstanceRequirements

Pour utiliser la sélection d'instance basée sur les attributs, vous devez inclure la structure `InstanceRequirements` dans votre configuration de flotte et spécifier les attributs souhaités pour les instances de la flotte.

Dans l'exemple précédent, les attributs d'instance suivants sont spécifiés :

- `VCpuCount` : les types d'instances doivent comporter au minimum 2 et au maximum 8 vCPU.
- `MemoryMiB` : les types d'instance doivent disposer d'un maximum de 10 240 Mio de mémoire. Un minimum de 0 indique qu'il n'y a pas de limite minimale.
- `MemoryGiBPerVCpu` : les types d'instance doivent disposer d'un maximum de 10 000 Gio de mémoire par vCPU. Le paramètre `Min` est facultatif. En l'omettant, vous n'indiquez aucune limite minimale.

TargetCapacityUnitType

Le paramètre `TargetCapacityUnitType` spécifie l'unité de la capacité cible. Dans cet exemple, la capacité cible est 5000 et le type d'unité de capacité cible est `vcpu`, qui spécifient ensemble une

capacité cible souhaitée de 5 000 vCPU. Le parc d'instances Spot lancera suffisamment d'instances pour que le nombre total de vCPU dans la flotte soit de 5 000.

Configuration valide : modèle de lancement unique avec plusieurs InstanceRequirements

La configuration suivante est valide. Elle contient un modèle de lancement et une structure Overrides contenant deux structures InstanceRequirements. Les attributs spécifiés dans InstanceRequirements sont valides car les valeurs ne se chevauchent pas. La première structure InstanceRequirements spécifie une VCpuCount de 0 à 2 vCPU, tandis que la seconde structure InstanceRequirements spécifie 4 à 8 vCPU.

```
{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchTemplateConfigs": [
      {
        "LaunchTemplateSpecification": {
          "LaunchTemplateName": "MyLaunchTemplate",
          "Version": "1"
        },
        "Overrides": [
          {
            "InstanceRequirements": {
              "VCpuCount": {
                "Min": 0,
                "Max": 2
              },
              "MemoryMiB": {
                "Min": 0
              }
            }
          }
        ],
        {
          "InstanceRequirements": {
            "VCpuCount": {
              "Min": 4,
              "Max": 8
            },
            "MemoryMiB": {
              "Min": 0
            }
          }
        }
      ]
    }
  }
}
```

```

        }
      }
    ]
  }
],
"TargetCapacity": 1,
"OnDemandTargetCapacity": 0,
"Type": "maintain"
}
}

```

Configuration valide : deux modèles de lancement, chacun avec des remplacements

La configuration suivante est valide. Elle contient deux modèles de lancement, chacun contenant une structure `Overrides` contenant une structure `InstanceRequirements`. Cette configuration est utile pour la prise en charge des architectures arm et x86 au sein de la même flotte.

```

{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchTemplateConfigs": [
      {
        "LaunchTemplateSpecification": {
          "LaunchTemplateName": "armLaunchTemplate",
          "Version": "1"
        },
        "Overrides": [
          {
            "InstanceRequirements": {
              "VCpuCount": {
                "Min": 0,
                "Max": 2
              },
              "MemoryMiB": {
                "Min": 0
              }
            }
          }
        ],
        {

```

```

    "LaunchTemplateSpecification": {
      "LaunchTemplateName": "x86LaunchTemplate",
      "Version": "1"
    },
    "Overrides": [
      {
        "InstanceRequirements": {
          "VCpuCount": {
            "Min": 0,
            "Max": 2
          },
          "MemoryMiB": {
            "Min": 0
          }
        }
      }
    ]
  },
  "TargetCapacity": 1,
  "OnDemandTargetCapacity": 0,
  "Type": "maintain"
}
}

```

Configuration valide : uniquement **InstanceRequirements** est spécifié, les valeurs d'attribut ne se chevauchent pas

La configuration suivante est valide. Elle contient deux structures `LaunchTemplateSpecification`, chacune avec un modèle de lancement et une structure `Overrides` contenant une structure `InstanceRequirements`. Les attributs spécifiés dans `InstanceRequirements` sont valides car les valeurs ne se chevauchent pas. La première structure `InstanceRequirements` spécifie une `VCpuCount` de 0 à 2 vCPU, tandis que la seconde structure `InstanceRequirements` spécifie 4 à 8 vCPU.

```

{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchTemplateConfigs": [

```

```
{
  "LaunchTemplateSpecification": {
    "LaunchTemplateName": "MyLaunchTemplate",
    "Version": "1"
  },
  "Overrides": [
    {
      "InstanceRequirements": {
        "VCpuCount": {
          "Min": 0,
          "Max": 2
        },
        "MemoryMiB": {
          "Min": 0
        }
      }
    }
  ],
},
{
  "LaunchTemplateSpecification": {
    "LaunchTemplateName": "MyOtherLaunchTemplate",
    "Version": "1"
  },
  "Overrides": [
    {
      "InstanceRequirements": {
        "VCpuCount": {
          "Min": 4,
          "Max": 8
        },
        "MemoryMiB": {
          "Min": 0
        }
      }
    }
  ]
},
],
"TargetCapacity": 1,
"OnDemandTargetCapacity": 0,
"Type": "maintain"
}
```

```
}
```

Configuration non valide : les **Overrides** contiennent **InstanceRequirements** et **InstanceType**

La configuration suivante n'est pas valide. La structure Overrides contient à la fois InstanceRequirements et InstanceType. Pour les Overrides, vous pouvez spécifier InstanceRequirements ou InstanceType, mais pas les deux.

```
{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchTemplateConfigs": [
      {
        "LaunchTemplateSpecification": {
          "LaunchTemplateName": "MyLaunchTemplate",
          "Version": "1"
        },
        "Overrides": [
          {
            "InstanceRequirements": {
              "VCpuCount": {
                "Min": 0,
                "Max": 2
              },
              "MemoryMiB": {
                "Min": 0
              }
            }
          },
          {
            "InstanceType": "m5.large"
          }
        ]
      }
    ],
    "TargetCapacity": 1,
    "OnDemandTargetCapacity": 0,
    "Type": "maintain"
  }
}
```

Configuration non valide : deux **Overrides** contiennent **InstanceRequirements** et **InstanceType**

La configuration suivante n'est pas valide. Les structures Overrides contiennent à la fois InstanceRequirements et InstanceType. Vous pouvez spécifier InstanceRequirements ou InstanceType, mais pas les deux, même s'ils se trouvent dans différentes structures Overrides.

```
{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchTemplateConfigs": [
      {
        "LaunchTemplateSpecification": {
          "LaunchTemplateName": "MyLaunchTemplate",
          "Version": "1"
        },
        "Overrides": [
          {
            "InstanceRequirements": {
              "VCpuCount": {
                "Min": 0,
                "Max": 2
              },
              "MemoryMiB": {
                "Min": 0
              }
            }
          }
        ]
      }
    ],
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "MyOtherLaunchTemplate",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "m5.large"
        }
      ]
    }
  ]
}
```

```

    }
  ],
  "TargetCapacity": 1,
  "OnDemandTargetCapacity": 0,
  "Type": "maintain"
}
}

```

Configuration non valide : chevauchement des valeurs d'attribut

La configuration suivante n'est pas valide. Les deux structures `InstanceRequirements` contiennent chacune `"VCpuCount": {"Min": 0, "Max": 2}`. Les valeurs de ces attributs se chevauchent, ce qui entraîne des groupes de capacités en double.

```

{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchTemplateConfigs": [
      {
        "LaunchTemplateSpecification": {
          "LaunchTemplateName": "MyLaunchTemplate",
          "Version": "1"
        },
        "Overrides": [
          {
            "InstanceRequirements": {
              "VCpuCount": {
                "Min": 0,
                "Max": 2
              },
              "MemoryMiB": {
                "Min": 0
              }
            }
          },
          {
            "InstanceRequirements": {
              "VCpuCount": {
                "Min": 0,
                "Max": 2
              }
            }
          }
        ]
      }
    ]
  }
}

```

```

        "MemoryMiB": {
            "Min": 0
        }
    }
}
],
"TargetCapacity": 1,
"OnDemandTargetCapacity": 0,
"Type": "maintain"
}
}

```

Aperçu des types d'instances avec des attributs spécifiés

Vous pouvez utiliser la AWS CLI commande [get-instance-types-from-instance-requirements](#) pour prévisualiser les types d'instances qui correspondent aux attributs que vous spécifiez. Cela est particulièrement utile pour déterminer les attributs à spécifier dans la configuration de votre demande sans lancer d'instance. Notez que la commande ne prend pas en compte la capacité disponible.

Pour prévisualiser une liste de types d'instances en spécifiant des attributs à l'aide du AWS CLI

1. (Facultatif) Pour générer tous les attributs possibles pouvant être spécifiés, utilisez la commande [get-instance-types-from-instance-requirements](#) et le paramètre `--generate-cli-skeleton`. Vous pouvez éventuellement rediriger la sortie vers un fichier pour l'enregistrer à l'aide de `input > attributes.json`.

```

aws ec2 get-instance-types-from-instance-requirements \
  --region us-east-1 \
  --generate-cli-skeleton input > attributes.json

```

Sortie attendue

```

{
  "DryRun": true,
  "ArchitectureTypes": [
    "i386"
  ],
  "VirtualizationTypes": [

```

```
    "hvm"
  ],
  "InstanceRequirements": {
    "VCpuCount": {
      "Min": 0,
      "Max": 0
    },
    "MemoryMiB": {
      "Min": 0,
      "Max": 0
    },
    "CpuManufacturers": [
      "intel"
    ],
    "MemoryGiBPerVCpu": {
      "Min": 0.0,
      "Max": 0.0
    },
    "ExcludedInstanceTypes": [
      ""
    ],
    "InstanceGenerations": [
      "current"
    ],
    "SpotMaxPricePercentageOverLowestPrice": 0,
    "OnDemandMaxPricePercentageOverLowestPrice": 0,
    "BareMetal": "included",
    "BurstablePerformance": "included",
    "RequireHibernateSupport": true,
    "NetworkInterfaceCount": {
      "Min": 0,
      "Max": 0
    },
    "LocalStorage": "included",
    "LocalStorageTypes": [
      "hdd"
    ],
    "TotalLocalStorageGB": {
      "Min": 0.0,
      "Max": 0.0
    },
    "BaselineEbsBandwidthMbps": {
      "Min": 0,
      "Max": 0
    }
  }
}
```

```
    },
    "AcceleratorTypes": [
      "gpu"
    ],
    "AcceleratorCount": {
      "Min": 0,
      "Max": 0
    },
    "AcceleratorManufacturers": [
      "nvidia"
    ],
    "AcceleratorNames": [
      "a100"
    ],
    "AcceleratorTotalMemoryMiB": {
      "Min": 0,
      "Max": 0
    },
    "NetworkBandwidthGbps": {
      "Min": 0.0,
      "Max": 0.0
    },
    "AllowedInstanceTypes": [
      ""
    ]
  },
  "MaxResults": 0,
  "NextToken": ""
}
```

2. Créez un fichier de configuration JSON à l'aide de la sortie de l'étape précédente et configurez-le comme suit :

Note

Vous devez fournir des valeurs pour `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` et `MemoryMiB`. Vous pouvez omettre les autres attributs. Lorsqu'ils sont omis, les valeurs par défaut sont utilisées.

Pour obtenir une description de chaque attribut et de leurs valeurs par défaut, consultez [get-instance-types-from-instance-requirements](#) dans la Référence des commandes en ligne Amazon EC2.

- a. Pour `ArchitectureTypes`, spécifiez un ou plusieurs types d'architecture de processeur.
 - b. Pour `VirtualizationTypes`, spécifiez un ou plusieurs types de virtualisation.
 - c. Pour `VCpuCount`, spécifiez le nombre minimum et maximum de vCPU. Pour ne spécifier aucune limite minimale, pour `Min`, spécifiez `0`. Pour ne spécifier aucune limite maximale, omettez le paramètre `Max`.
 - d. Pour `MemoryMiB`, spécifiez la quantité minimale et maximale de mémoire en Mio. Pour ne spécifier aucune limite minimale, pour `Min`, spécifiez `0`. Pour ne spécifier aucune limite maximale, omettez le paramètre `Max`.
 - e. Vous pouvez éventuellement spécifier un ou plusieurs autres attributs pour limiter davantage la liste des types d'instance renvoyés.
3. Pour afficher un aperçu des types d'instance qui possèdent les attributs que vous avez spécifiés dans le fichier JSON, utilisez la commande [get-instance-types-from-instance-requirements](#) et spécifiez le nom et le chemin d'accès à votre fichier JSON à l'aide du paramètre `--cli-input-json`. Vous pouvez éventuellement formater la sortie pour qu'elle apparaisse dans un format de tableau.

```
aws ec2 get-instance-types-from-instance-requirements \  
  --cli-input-json file://attributes.json \  
  --output table
```

Fichier `attributes.json` d'exemple

Dans cet exemple, les attributs requis sont inclus dans le fichier JSON. Ils sont `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` et `MemoryMiB`. En outre, l'attribut facultatif `InstanceGenerations` est également inclus. Notez que pour `MemoryMiB`, la valeur `Max` peut être omise pour indiquer qu'aucune limite n'est applicable.

```
{  
  "ArchitectureTypes": [  
    "x86_64"  
  ],  
  "VirtualizationTypes": [  
    "hvm"  
  ],  
  "InstanceRequirements": {  
    "VCpuCount": {
```

```

        "Min": 4,
        "Max": 6
    },
    "MemoryMiB": {
        "Min": 2048
    },
    "InstanceGenerations": [
        "current"
    ]
}
}

```

Exemple de sortie

```

-----
|GetInstanceTypesFromInstanceRequirements|
+-----+
||           InstanceTypes           ||
|+-----+|
||           InstanceType           ||
|+-----+|
|| c4.xlarge                         ||
|| c5.xlarge                         ||
|| c5a.xlarge                        ||
|| c5ad.xlarge                       ||
|| c5d.xlarge                        ||
|| c5n.xlarge                        ||
|| c6a.xlarge                        ||
|| ...                               ||

```

- Après avoir identifié les types d'instance qui répondent à vos besoins, prenez note des attributs d'instance que vous avez utilisés afin que vous puissiez les utiliser lors de la configuration de votre demande de flotte.

À la demande dans la demande de parc d'instances Spot

Pour garantir que vous avez toujours la capacité d'instance, vous pouvez inclure une demande de capacité à la demande dans votre demande de parc d'instances Spot . Dans votre demande de parc d'instances Spot , vous spécifiez votre capacité cible souhaitée et quelle quantité de la capacité doit être à la demande. Le solde inclut la capacité Spot qui est lancée si une capacité et une disponibilité Amazon EC2 sont disponibles. Par exemple, si dans votre demande de parc d'instances Spot, vous

spécifiez la capacité cible de 10 et la capacité à la demande de 8, Amazon EC2 lance 8 unités de capacité à la demande et 2 unités de capacité ($10 - 8 = 2$) comme unités Spot.

Hiérarchiser les types d'instance pour la capacité à la demande

Lorsque le parc d'instances Spot essaie de traiter l'affectation de capacité à la demande, il lance par défaut le type d'instance dont le prix est le plus bas en premier. Si `OnDemandAllocationStrategy` a pour valeur `prioritized`, le parc d'instances Spot utilise la priorité pour déterminer quel type d'instance utiliser en premier afin de traiter l'affectation de capacité à la demande.

La priorité est affectée au remplacement du modèle de lancement, et la priorité la plus élevée est lancée en premier.

Exemple : donner la priorité aux types d'instance

Dans cet exemple, vous configurez trois dérogations au modèle de lancement, chacune avec un type d'instance différent.

Le prix à la demande des types d'instance varie. Voici les types d'instance utilisés dans cet exemple, classés par ordre de prix, en commençant par le type d'instance le moins cher :

- `m4.large` : le moins cher
- `m5.large`
- `m5a.large`

Si vous n'utilisez pas la priorité pour déterminer l'ordre, la flotte remplit la capacité à la demande en commençant par le type d'instance le moins cher.

Toutefois, supposons que vous avez des instances réservées `m5.large` inutilisées que vous voulez utiliser en premier. Vous pouvez définir la priorité de remplacement du modèle de lancement afin que les types d'instance soient utilisés dans l'ordre de priorité, comme suit :

- `m5.large` : priorité 1
- `m4.large` : priorité 2
- `m5a.large` : priorité 3

Rééquilibrage de la capacité

Vous pouvez configurer un parc d'instances Spot pour lancer une instance Spot de remplacement lorsqu'Amazon EC2 émet une recommandation de rééquilibrage pour vous avertir qu'une instance Spot présente un risque d'interruption élevé. Le rééquilibrage de capacité vous permet de maintenir la disponibilité de la charge de travail en augmentant de manière proactive votre flotte avec une nouvelle instance Spot avant qu'une instance en cours d'exécution ne soit interrompue par Amazon EC2. Pour plus d'informations, consultez [Recommandations de rééquilibrage des instances EC2](#).

Pour configurer le parc d'instances Spot pour lancer une instance Spot de remplacement, vous pouvez utiliser la console Amazon EC2 ou la AWS CLI.

- Console Amazon EC2 : vous devez cocher la case Rééquilibrage de capacité lors de la création du parc d'instances Spot. Pour plus d'informations, consultez l'étape 6.d dans [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#).
- AWS CLI: utilisez la commande [request-spot-fleet](#) et les paramètres pertinents dans la structure `SpotMaintenanceStrategies`. Pour plus d'informations, consultez l'[exemple de configuration de lancement](#).

Limites

- Le rééquilibrage de capacité est disponible uniquement pour les flottes de type `maintain`.
- Lorsque la flotte est en cours d'exécution, vous ne pouvez pas modifier le paramètre Rééquilibrage de capacité. Pour modifier le paramètre Rééquilibrage de capacité, vous devez supprimer la flotte et en créer un nouveau.

Options de configuration

La `ReplacementStrategy` pour le parc d'instances Spot prend en charge les deux valeurs suivantes :

`launch-before-terminate`

Amazon EC2 met fin aux instances Spot qui reçoivent une notification de rééquilibrage après le lancement de nouvelles instances Spot de remplacement. Quand vous spécifiez `launch-before-terminate`, vous devez également spécifier une valeur pour `termination-delay`. Une fois les nouvelles instances de remplacement lancées, Amazon EC2 attend la durée du

`termination-delay`, puis résilie les anciennes instances. Pour `termination-delay`, le minimum est de 120 secondes (2 minutes) et le maximum est de 7 200 secondes (2 heures).

Nous vous recommandons d'utiliser `launch-before-terminate` uniquement si vous pouvez prédire la durée de la procédure d'arrêt de votre instance. Cela garantit que les anciennes instances ne sont résiliées qu'une fois les procédures d'arrêt terminées. Notez qu'Amazon EC2 peut interrompre les anciennes instances avec un avertissement de deux minutes avant le `termination-delay`.

launch

Amazon EC2 lance des instances Spot de remplacement lorsqu'une notification de rééquilibrage est émise pour les instances Spot existantes. Amazon EC2 ne résilie pas les instances qui reçoivent une notification de rééquilibrage. Vous pouvez résilier les anciennes instances ou les laisser en cours d'exécution. Toutes les instances en cours d'exécution vous sont facturées.

Considérations

Si vous configurez un parc d'instances Spot pour le rééquilibrage de capacité, tenez compte des points suivants :

Fournissez autant de groupes de capacité Spot que possible dans la demande

Configurez votre parc d'instances Spot pour utiliser plusieurs types d'instance et zones de disponibilité. Cela permet de lancer des instances Spot dans divers groupes de capacité Spot. Pour plus d'informations, consultez [Soyez flexible en ce qui concerne les types d'instance et les zones de disponibilité](#).

Éviter un risque élevé d'interruption des instances Spot de remplacement

Pour éviter un risque élevé d'interruption, nous recommandons la stratégie `capacityOptimizedPrioritized` d'allocation `capacityOptimized` or. Ces stratégies garantissent que les instances Spot de remplacement sont lancées dans les groupes de capacité Spot optimaux et sont donc moins susceptibles d'être interrompues dans un proche avenir. Pour plus d'informations, consultez [Utiliser la stratégie d'allocation optimisée pour le prix et la capacité](#).

Amazon EC2 ne lancera une nouvelle instance que si la disponibilité est identique ou meilleure

L'un des objectifs du rééquilibrage de capacité est d'améliorer la disponibilité d'une instance Spot. Si une instance Spot existante reçoit une recommandation de rééquilibrage, Amazon EC2 ne lancera une nouvelle instance que si la nouvelle instance offre une disponibilité supérieure ou égale à celle de l'instance existante. Si le risque d'interruption d'une nouvelle instance est plus

important que celui de l'instance existante, Amazon EC2 ne lancera pas de nouvelle instance. Amazon EC2 continuera toutefois à évaluer les groupes de capacité Spot et lancera une nouvelle instance si la disponibilité s'améliore.

Il est possible que votre instance existante soit interrompue sans qu'Amazon EC2 ne lance une nouvelle instance de manière proactive. Lorsque cela se produit, Amazon EC2 essaiera de lancer une nouvelle instance, que la nouvelle instance présente un risque d'interruption élevé ou non.

Le rééquilibrage de capacité n'augmente pas le taux d'interruption de votre instance Spot

Lorsque vous activez le rééquilibrage de la capacité, cette action n'augmente pas votre [Taux d'interruption d'instance Spot](#). (Le nombre d'instances Spot qui sont récupérées lorsqu'Amazon EC2 doit récupérer de l'espace. Toutefois, si le rééquilibrage de la capacité détecte une potentielle interruption d'instance, Amazon EC2 essaiera instantanément de lancer une nouvelle instance. En résultat, un nombre supérieur d'instances pourraient être remplacées, comparativement au scénario où vous attendriez qu'Amazon EC2 lance une nouvelle instance après l'interruption de l'instance à risque.

Bien que vous puissiez remplacer davantage d'instances lorsque le rééquilibrage de la capacité est activé, vous gagnerez à faire preuve de proactivité que de réactivité en disposant de plus de temps d'action avant l'interruption de vos instances. En général, après un [Avis d'interruption d'instance Spot](#), vous ne disposez que deux minutes pour arrêter correctement votre instance. Etant donné que le rééquilibrage de la capacité lance une nouvelle instance à l'avance, vous donnez aux processus existants de meilleures chances de se terminer sur votre instance à risque. Vous pouvez démarrer les procédures d'arrêt de votre instance et empêcher la planification de nouveaux travaux sur votre instance à risque. Vous pouvez également commencer à préparer l'instance nouvellement lancée afin de prendre le contrôle de l'application. Grâce au remplacement proactif de Capacity Rebalancing, vous bénéficiez d'une continuité.

À titre d'exemple théorique pour démontrer les risques et les avantages liés au rééquilibrage des capacités, considérez le scénario suivant :

- 14 h 00 : une recommandation de rééquilibrage est reçue pour l'instance-A, et Amazon EC2 essaie instantanément de lancer une Instance-B de remplacement, ce qui vous laisse le temps de démarrer vos procédures d'arrêt.*
- 14 h 30 — Une recommandation de rééquilibrage est reçue pour l'instance-B, remplacée par Instance-C, ce qui vous donne le temps de démarrer vos procédures d'arrêt. *
- 14 h 32 — Si le rééquilibrage de la capacité n'était pas activé, et si un avis d'interruption d'instance Spot avait été reçu à 14h32 pour l'instance-A, vous n'auriez disposé que de deux minutes pour agir. Cependant, l'instance-A aurait été en cours d'exécution jusqu'à ce moment.

* Si `launch-before-terminate` est spécifié, Amazon EC2 mettra fin à l'instance à risque après la mise en ligne de l'instance de remplacement.

Amazon EC2 peut lancer de nouvelles instances Spot de remplacement jusqu'à ce que la capacité exécutée représente le double de la capacité cible

Lorsqu'un parc d'instances Spot est configuré pour le rééquilibrage de capacité, Amazon EC2 tente de lancer une nouvelle instance Spot de remplacement pour chaque instance Spot qui reçoit une recommandation de rééquilibrage. Une fois qu'une instance Spot reçoit une recommandation de rééquilibrage, elle n'est plus comptabilisée dans la capacité exécutée. Selon la stratégie de remplacement, Amazon EC2 résilie l'instance après un délai de terminaison préconfiguré ou la laisse en cours d'exécution. Cela vous donne la possibilité d'effectuer des [actions de rééquilibrage](#) sur l'instance.

Si votre flotte atteint le double de sa capacité cible, il cesse de lancer de nouvelles instances de remplacement même si les instances de remplacement elles-mêmes reçoivent une recommandation de rééquilibrage.

Par exemple, vous créez un parc d'instances Spot avec une capacité cible de 100 instances Spot. Toutes les instances Spot reçoivent une recommandation de rééquilibrage, ce qui entraîne le lancement par Amazon EC2 de 100 instances Spot de remplacement. Cela augmente le nombre d'instances Spot exécutées à 200, soit le double de la capacité cible. Certaines instances de remplacement reçoivent une recommandation de rééquilibrage, mais aucune autre instance de remplacement n'est lancée car la flotte ne peut pas dépasser le double de sa capacité cible.

Notez que vous êtes facturé pour toutes les instances pendant qu'elles sont en cours d'exécution.

Nous vous recommandons de configurer le parc d'instances Spot afin qu'il résilie les instances Spot qui reçoivent une recommandation de rééquilibrage

Si vous configurez votre parc d'instances Spot pour le rééquilibrage de capacité, nous vous recommandons de choisir `launch-before-terminate` avec un délai de résiliation approprié uniquement si vous pouvez prédire la durée de la procédure d'arrêt de votre instance. Cela garantit que les anciennes instances ne sont résiliées qu'une fois les procédures d'arrêt terminées.

Si vous choisissez de résilier vous-même les instances recommandées pour le rééquilibrage, nous vous recommandons de surveiller le signal de recommandation de rééquilibrage reçu par les instances Spot de la flotte. En surveillant le signal, vous pouvez effectuer rapidement des [actions de rééquilibrage](#) sur les instances concernées avant qu'Amazon EC2 ne les interrompe, puis vous

pouvez les résilier manuellement. Si vous ne résiliez pas les instances, vous continuez à les payer pendant qu'elles sont en cours d'exécution. Amazon EC2 ne résilie pas automatiquement les instances qui reçoivent une recommandation de rééquilibrage.

Vous pouvez configurer des notifications à l'aide d'Amazon EventBridge ou des métadonnées d'instance. Pour plus d'informations, consultez [Surveiller les signaux de recommandation de rééquilibrage](#).

Le parc d'instances Spot ne prend pas en compte les instances qui reçoivent une recommandation de rééquilibrage lors du calcul de la capacité exécutée pendant la diminution ou l'augmentation

Si votre parc d'instances Spot est configuré pour le rééquilibrage de capacité et que vous modifiez la capacité cible pour qu'elle soit diminuée ou augmentée, la flotte ne comptabilise pas les instances marquées pour rééquilibrage dans le cadre de la capacité exécutée, comme suit :

- Mise à l'échelle horizontale : si vous diminuez la capacité cible souhaitée, Amazon EC2 résilie les instances qui ne sont pas marquées pour rééquilibrage tant que la capacité souhaitée n'est pas atteinte. Les instances marquées pour rééquilibrage ne sont pas prises en compte dans la capacité exécutée.

Par exemple, vous créez un parc d'instances Spot avec une capacité cible de 100 instances Spot, 10 instances reçoivent une recommandation de rééquilibrage, Amazon EC2 lance alors 10 nouvelles instances de remplacement, ce qui donne une capacité exécutée de 110 instances. Vous réduisez ensuite la capacité cible à 50 (mise à l'échelle horizontale), mais la capacité exécutée est en fait de 60 instances car les 10 instances marquées pour rééquilibrage ne sont pas résiliées par Amazon EC2. Vous devez résilier manuellement ces instances, ou vous pouvez les laisser en cours d'exécution.

- Montée en puissance : si vous augmentez la capacité cible souhaitée, Amazon EC2 lance de nouvelles instances tant que la capacité souhaitée n'est pas atteinte. Les instances marquées pour rééquilibrage ne sont pas prises en compte dans la capacité exécutée.

Par exemple, vous créez un parc d'instances Spot avec une capacité cible de 100 instances Spot, 10 instances reçoivent une recommandation de rééquilibrage, Amazon EC2 lance alors 10 nouvelles instances de remplacement, ce qui donne une capacité exécutée de 110 instances. Vous augmentez ensuite la capacité cible à 200 (augmentation), mais la capacité exécutée est en fait de 210 instances car les 10 instances marquées pour rééquilibrage ne sont pas comptabilisées par la flotte comme faisant partie de la capacité cible. Vous devez résilier manuellement ces instances, ou vous pouvez les laisser en cours d'exécution.

Remplacements du prix Spot

Chaque parc d'instances Spot peut inclure un prix maximum global ou utiliser la valeur par défaut (prix à la demande). Le parc d'instances Spot utilise ce prix comme prix maximum par défaut pour chacune de ses spécifications de lancement.

Si vous le souhaitez, vous pouvez également spécifier un prix maximum dans une ou plusieurs spécifications de lancement. Ce prix est propre à la spécification de lancement. Si une spécification de lancement comprend un prix spécifique, le parc d'instances Spot utilise ce prix maximum à la place du prix maximum global. Toute autre spécification de lancement qui ne comprend pas de prix maximum spécifique continue à utiliser le prix maximum global.

Contrôle des dépenses

Le parc d'instances Spot arrête le lancement des instances une fois que la capacité cible ou le montant maximum que vous êtes prêt à payer a été atteint. Pour contrôler le montant payé par heure pour votre parc, vous pouvez spécifier `SpotMaxTotalPrice` pour Instances Spot et `OnDemandMaxTotalPrice` pour Instances à la demande. Une fois le prix maximum total atteint, le parc d'instances Spot arrête de lancer des instances même si la capacité cible n'a pas été atteinte.

Les exemples suivants montrent deux manières de le faire. Dans le premier, le parc d'instances Spot arrête de lancer des instances une fois la capacité cible atteinte. Dans le deuxième, le parc d'instances Spot arrête le lancement des instances une fois le montant maximum que vous êtes prêt à payer atteint.

Exemple : Arrêt du lancement des instances lorsque la capacité cible est atteinte

Prenons l'exemple d'une demande pour `m4.large` Instances à la demande, avec :

- Prix à la demande : 0,10 USD par heure
- `OnDemandTargetCapacity` : 10
- `OnDemandMaxTotalPrice` : 1,50 USD

Le parc d'instances Spot lance 10 instances à la demande car le total de 1 USD (10 instances x 0,10 USD) ne dépasse pas le `OnDemandMaxTotalPrice` de 1,50 USD.

Exemple : Arrêt du lancement des instances lorsque le prix total maximum est atteint

Prenons l'exemple d'une demande pour `m4.large` Instances à la demande, avec :

- Prix à la demande : 0,10 USD par heure
- `OnDemandTargetCapacity` : 10
- `OnDemandMaxTotalPrice` : 0,80 USD

Si le parc d'instances Spot lance la capacité cible à la demande (10 instances à la demande), le coût total par heure est de 1 USD. Ce montant est supérieur à celui (0,80 USD) spécifié pour `OnDemandMaxTotalPrice`. Afin d'éviter de dépenser plus que vous le souhaitez, le parc d'instances Spot lance uniquement 8 instances à la demande (ce qui est inférieur à la capacité cible à la demande) car le lancement d'instances supplémentaires dépasserait le `OnDemandMaxTotalPrice`.

Pondération d'instance de parc d'instances Spot

Lorsque vous demandez un parc d'Instances Spot, vous pouvez définir les unités de capacité que chaque type d'instance apporterait aux performances de votre application et ajuster votre prix maximum pour chaque groupe de capacités Spot en conséquence à l'aide de la pondération d'instance.

Par défaut, le prix que vous spécifiez représente le prix par heure d'instance. Lorsque vous utilisez la fonction de pondération d'instance, le prix que vous spécifiez correspond au prix par heure d'unité. Vous pouvez calculer le prix par heure d'unité en divisant le prix pour un type d'instance par le nombre d'unités qu'il représente. Le parc d'instances Spot calcule le nombre d'instances Spot à lancer en divisant la capacité cible par la pondération d'instance. Si le résultat n'est pas un nombre entier, le parc d'instances Spot l'arrondit à l'entier suivant afin que la taille de votre flotte ne soit pas inférieure à sa capacité cible. Le parc d'instances Spot peut sélectionner n'importe quel groupe indiqué dans votre spécification de lancement, même si la capacité des instances lancées dépasse la capacité cible demandée.

Les tableaux suivants présentent des exemples de calculs afin de déterminer le prix par unité pour une demande de parc d'instances Spot ayant une capacité cible de 10.

Type d'instance	Pondération de l'instance	Prix par heure d'instance	Prix par heure d'unité	Nombre d'instances lancées
r3.xlarge	2	0,05 USD	0,025	5

Type d'instance	Pondération de l'instance	Prix par heure d'instance	Prix par heure d'unité	Nombre d'instances lancées
			(0,05 divisé par 2)	(10 divisé par 2)
Type d'instance	Pondération de l'instance	Prix par heure d'instance	Prix par heure d'unité	Nombre d'instances lancées
r3.xlarge	8	0,10 USD	0,0125 (0,10 divisé par 8)	2 (10 divisé par 8, résultat arrondi)

Utilisez la pondération d'instance de parc d'instances Spot comme suit, afin d'attribuer la capacité cible que vous voulez dans les groupes selon le prix par unité le plus bas au moment de l'exécution :

1. Définissez la capacité cible de votre parc d'instances Spot en instances (valeur par défaut) ou dans les unités de votre choix, par exemple les UC virtuelles, la mémoire, le stockage ou le débit.
2. Définissez le prix par unité.
3. Pour chaque configuration de lancement, spécifiez la pondération, c'est-à-dire le nombre d'unités du type d'instance par rapport à la capacité cible.

Exemple de pondération d'instance

Prenons l'exemple d'une demande de parc d'instances Spot avec la configuration suivante :

- Capacité cible de 24
- Spécification de lancement avec le type d'instance r3.2xlarge et une pondération de 6
- Spécification de lancement avec le type d'instance c3.xlarge et une pondération de 5

La pondération correspond au nombre d'unités du type d'instance par rapport à la capacité cible. Si la première spécification de lancement fournit le prix par unité le plus faible (prix pour `r3.xlarge` par heure d'instance divisé par 6), le parc d'instances Spot lance quatre de ces instances (24 divisé par 6).

Si la deuxième spécification de lancement fournit le prix par unité le plus bas (prix pour `c3.xlarge` par heure d'instance divisé par 5), le parc d'instances Spot lance cinq de ces instances (24 divisé par 5, résultat arrondi).

Pondération d'instance et stratégie d'allocation

Prenons l'exemple d'une demande de parc d'instances Spot avec la configuration suivante :

- Capacité cible de 30
- Spécification de lancement avec le type d'instance `c3.2xlarge` et une pondération de 8
- Spécification de lancement avec le type d'instance `m3.xlarge` et une pondération de 8
- Spécification de lancement avec le type d'instance `r3.xlarge` et une pondération de 8

Le parc d'instances Spot lancerait quatre instances (30 divisé par 8, résultat arrondi). Avec la politique `diversified`, le parc d'instances Spot lance une instance dans chacun des trois groupes, et lance la quatrième instance dans l'un des groupes ayant le prix par unité le plus bas.

Utilisation de flottes d'instances Spot

Pour utiliser un parc d'instances Spot , vous devez créer une demande de parc d'instances Spot comprenant la capacité cible, une part à la demande facultative, une ou plusieurs spécifications de lancement pour les instances et le prix maximum que vous êtes prêt à payer. La demande de flotte d'instances doit inclure une spécification de lancement paramétrant les informations dont la flotte d'instances a besoin pour lancer une instance, par exemple une AMI, un type d'instance, un sous-réseau ou une zone de disponibilité, et un ou plusieurs groupes de sécurité.

Si votre flotte d'instances inclut des instances Spot, Amazon EC2 tente de maintenir la capacité cible de votre flotte d'instances au fur et à mesure de l'évolution des prix Spot.

Il n'est pas possible de modifier la capacité cible d'une demande unique une fois qu'elle a été soumise. Pour modifier la capacité cible, annulez la demande et soumettez-en une nouvelle.

Une demande de parc d'instances Spot reste active jusqu'à ce qu'elle arrive à expiration ou que vous l'annuliez. Lorsque vous annulez une demande de parc d'instances Spot, vous pouvez spécifier si l'annulation de votre demande de parc d'instances Spot résilie les instances Spot de votre flotte.

Table des matières

- [État des demandes de parc d'instances Spot](#)
- [Vérifications de l'état du parc d'instances Spot](#)
- [Autorisations du parc d'instances Spot](#)
- [Créer une Spot Fleet request](#)
- [Étiqueter un parc d'instances Spot](#)
- [Décrire votre parc d'instances Spot](#)
- [Modifier une demande de parc d'instances Spot](#)
- [Annulation d'une demande de parc d'instances Spot](#)

État des demandes de parc d'instances Spot

Une demande de parc d'instances Spot peut avoir l'un des états suivants :

- **submitted** : la demande de parc d'instances Spot est en cours d'évaluation et Amazon EC2 se prépare à lancer le nombre cible d'instances. Si une requête dépasse les limites du parc d'instances Spot, elle est annulée immédiatement.
- **active** : la demande de parc d'instances Spot a été validée et Amazon EC2 tente de conserver le nombre cible d'instances Spot en cours d'exécution. La demande conserve cet état jusqu'à ce qu'elle soit modifiée ou annulée.
- **modifying** : la demande de parc d'instances Spot est en cours de modification. La demande conserve cet état jusqu'à ce que la modification soit totalement traitée ou que le parc d'instances Spot soit annulé. Il n'est pas possible de modifier une demande (request) unique, et cet état ne s'applique pas à ce type de demande d'instance Spot.
- **cancelled_running** : le parc d'instances Spot est annulé et ne lance pas d'instances Spot supplémentaires. Ses instances Spot existantes continuent de s'exécuter jusqu'à ce qu'elles soient interrompues ou mises hors service. La demande conserve cet état jusqu'à ce que toutes les instances soient interrompues ou mises hors service.
- **cancelled_terminating** : le parc d'instances Spot est annulé et ses instances Spot sont résiliées. La demande conserve cet état jusqu'à ce que toutes les instances soient mises hors service.

- **cancelled** : le parc d'instances Spot est annulé et n'a aucune instance Spot en cours d'exécution. La demande de parc d'instances Spot est supprimée deux jours après la résiliation de ses instances.

Vérifications de l'état du parc d'instances Spot

Le parc d'instances Spot vérifie l'intégrité des instances Spot de la flotte toutes les deux minutes. Le statut de l'état d'une instance est `healthy` ou `unhealthy`.

Le parc d'instances Spot détermine l'intégrité d'une instance en utilisant les vérifications d'état fournies par Amazon EC2. Une instance est déterminée comme `unhealthy` lorsque le contrôle du statut de l'instance ou de celui du système est `impaired` pendant trois surveillances consécutives de l'état. Pour plus d'informations, consultez [Contrôles de statut pour vos instances](#).

Vous pouvez configurer votre flotte pour qu'il remplace les instances Spot non saine. Après avoir activé le remplacement de la vérification de l'état, une instance Spot est remplacée lorsqu'elle est signalée comme `unhealthy`. Notez que la taille de la flotte peut être inférieure à sa capacité cible pendant quelques minutes pendant le remplacement d'une instance Spot non saine.

Prérequis

- Le remplacement de la vérification de l'état est pris en charge uniquement pour les Parcs d'instances Spot qui maintiennent une capacité cible (parcs de type `maintain`), pas pour les Parcs d'instances Spot uniques (parcs de type `request`).
- Le remplacement de la vérification de l'état n'est pris en charge que pour instances Spot. Cette fonctionnalité n'est pas prise en charge pour instances à la demande.
- Vous pouvez configurer votre parc d'instances Spot pour qu'il remplace les instances non saines au moment de sa création uniquement.
- Les utilisateurs peuvent utiliser le remplacement lié à la surveillance de l'état seulement s'ils sont autorisés à appeler l'action `ec2:DescribeInstanceStatus`.

Console

Pour configurer un parc d'instances Spot pour remplacer des instances Spot non saines en utilisant la console

1. Suivez les étapes permettant de créer un parc d'instances Spot . Pour plus d'informations, consultez [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#).
2. Pour configurer le parc de manière à remplacer les Instances Spot non saines, pour la vérification de l'état, choisissez Remplacer les instances non saines. Pour activer cette option, vous devez d'abord choisir Maintenir target capacity (Maintenir la capacité cible).

AWS CLI

Pour configurer un parc d'instances Spot pour remplacer des instances Spot non saines en utilisant la AWS CLI

1. Suivez les étapes permettant de créer un parc d'instances Spot . Pour plus d'informations, consultez [Créez une flotte de spots à l'aide du AWS CLI](#).
2. Pour configurer le parc de manière à remplacer les Instances Spot non saines, pour ReplaceUnhealthyInstances, entrez true.

Autorisations du parc d'instances Spot

Si vos utilisateurs sont appelés à créer ou à gérer un parc d'instances Spot, veillez à leur accorder les autorisations nécessaires.

Si vous utilisez la console Amazon EC2 pour créer un parc d'instances Spot , cela crée un rôle lié au service nommé AWSServiceRoleForEC2SpotFleet et AWSServiceRoleForEC2Spot, et un rôle nommé aws-ec2-spot-fleet-tagging-role qui octroie au parc d'instances Spot les autorisations de demander, de lancer, de résilier et d'étiqueter des ressources en votre nom. Si vous utilisez AWS CLI ou une API, vous devez vous assurer que ces rôles existent.

Suivez les instructions ci-dessous pour accorder les autorisations requises et créer les rôles.

Autorisations et rôles

- [Accorder des autorisations aux utilisateurs pour un parc instances Spot](#)
- [Rôle lié à un service pour un parc d'instances Spot](#)

- [Rôle lié à un service pour les instances Spot](#)
- [Rôle IAM pour l'étiquetage d'un parc d'instances Spot](#)

Accorder des autorisations aux utilisateurs pour un parc instances Spot

Si vos utilisateurs sont appelés à créer ou à gérer un parc d'instances Spot, veillez à leur accorder les autorisations nécessaires.

Pour créer une politique pour un parc d'instances Spot

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Politiques (Stratégies), puis Create policy (Créer une stratégie).
3. Sur la page Créer une stratégie, choisissez JSON, puis remplacez le texte par ce qui suit.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:RequestSpotFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequestHistory"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
```

```
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
}
]
```

L'exemple de politique précédent accorde à un utilisateur les autorisations requises pour la plupart des cas d'utilisation de parc d'instances Spot. Pour limiter l'utilisateur à des actions d'API données, spécifiez celles qui sont autorisées.

EC2 et API IAM requises

Les API suivantes doivent être incluses dans la politique :

- `ec2:RunInstances` : requis pour lancer des instances dans un parc d'instances Spot
- `ec2:CreateTags` : requis pour étiqueter la demande de parc d'instances Spot, les instances ou les volumes
- `iam:PassRole` : requis pour spécifier le rôle du parc d'instances Spot
- `iam:CreateServiceLinkedRole` : requis pour créer le rôle lié au service
- `iam:ListRoles` : requis pour énumérer les rôles IAM existants
- `iam:ListInstanceProfiles` : requis pour énumérer les profils d'instance existants

Important

Si vous spécifiez un rôle pour le profil d'instance IAM dans la spécification ou le modèle de lancement, vous devez accorder à l'utilisateur l'autorisation de transmettre le rôle au service. Pour ce faire, dans la stratégie IAM, incluez `"arn:aws:iam::*:role/IamInstanceProfile-role"` comme ressource pour l'action `iam:PassRole`. Pour plus d'informations, consultez la section [Octroi à un utilisateur des autorisations lui permettant de transmettre un rôle à un AWS service](#) dans le Guide de l'utilisateur IAM.

API de parc d'instances Spot

Ajoutez les actions d'API de parc d'instances Spot suivantes à votre politique, selon vos besoins :

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

API IAM facultatives

(Facultatif) Pour autoriser un utilisateur à créer des rôles ou des profils d'instances à l'aide de la console IAM, vous devez aussi ajouter les actions suivantes à la politique :

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Choisissez Examiner une stratégie.

5. Sur la page Review Policy (Vérifier la stratégie), saisissez un nom et une description pour la stratégie, puis choisissez Create policy (Créer une stratégie).

6. Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :
 - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.
 - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Rôle lié à un service pour un parc d'instances Spot

Amazon EC2 utilise des rôles liés à un service pour les autorisations requises pour appeler d'autres services AWS en votre nom. Un rôle lié à un service est un type unique de rôle IAM directement lié à un service. AWS Les rôles liés à un service constituent un moyen sécurisé de déléguer des autorisations aux AWS services, car seul le service lié peut assumer un rôle lié au service. Pour plus d'informations, consultez [Utilisation des rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Amazon EC2 utilise le rôle lié au service nommé `AWSServiceRoleForEC2SpotFleet` pour lancer et gérer des instances en votre nom.

Important

Si vous spécifiez une [AMI chiffrée](#) ou un instantané Amazon EBS chiffré dans votre parc de spots, vous devez accorder au `AWSServiceRoleForEC2SpotFleet` rôle l'autorisation d'utiliser le CMK afin qu'Amazon EC2 puisse lancer des instances en votre nom. Pour plus d'informations, consultez [Octroyer un accès aux CMK en vue de leur utilisation avec les AMI chiffrées et les instantanés EBS](#).

Autorisations accordées par `AWSServiceRoleForEC2SpotFleet`

Amazon EC2 permet `AWSServiceRoleForEC2SpotFleet` d'effectuer les actions suivantes :

- `ec2:RequestSpotInstances` - Demander des Instances Spot
- `ec2:RunInstances` - Lancer des instances
- `ec2:TerminateInstances` - Résilier des instances
- `ec2:DescribeImages` - Décrire des images Amazon Machine Images (AMI) pour les instances
- `ec2:DescribeInstanceStatus` - Décrire le statut des instances.
- `ec2:DescribeSubnets` - Décrire les sous-réseaux des instances

- `ec2:CreateTags` : ajouter des identifications à la demande de parc d'instances Spot, aux instances et aux volumes
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` - Ajouter les instances spécifiées à l'équilibreur de charge indiqué.
- `elasticloadbalancing:RegisterTargets` - Enregistrer les cibles spécifiées auprès du groupe cible indiqué.

Création du rôle lié à un service

Dans la plupart des cas, vous n'avez pas besoin de créer manuellement un rôle lié à un service. Amazon EC2 crée le rôle `AWSServiceRoleForEC2SpotFleet` au service la première fois que vous créez un parc de spots à l'aide de la console.

Si vous avez reçu une demande Spot Fleet active avant octobre 2017, date à laquelle Amazon EC2 a commencé à prendre en charge ce rôle lié à un service, Amazon EC2 a créé le rôle dans votre compte. `AWSServiceRoleForEC2SpotFleet` AWS Pour plus d'informations, consultez la section [Un nouveau rôle est apparu dans mon AWS compte](#) dans le guide de l'utilisateur IAM.

Si vous utilisez l'API AWS CLI ou une API pour créer un parc de spots, vous devez d'abord vous assurer que ce rôle existe.

Pour créer à `AWSServiceRoleForEC2SpotFleet` l'aide de la console

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Rôles.
3. Sélectionnez Create role (Créer un rôle).
4. Sur la page Select trusted entity (Sélectionner une entité de confiance), procédez comme suit :
 - a. Pour Type d'entité de confiance, choisissez Service AWS .
 - b. Sous Cas d'utilisation, pour Service ou cas d'utilisation, choisissez EC2.
 - c. Dans le cas d'utilisation, choisissez EC2 - Spot Fleet.
 - d. Choisissez Suivant.
5. Sur la page Ajouter des autorisations, sélectionnez Suivant.
6. Sur la page Nommer, vérifier et créer, choisissez Créer un rôle.

Pour créer à `AWSServiceRoleForEC2SpotFleet` l'aide du AWS CLI

Utilisez la commande [create-service-linked-role](#) comme suit.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Si vous n'avez plus besoin d'utiliser Spot Fleet, nous vous recommandons de supprimer le `AWSServiceRoleForEC2SpotFleet` rôle. Après sa suppression de votre compte, Amazon EC2 créera de nouveau le rôle si vous effectuez une demande de parc d'instances Spot à l'aide de la console. Pour plus d'informations, consultez [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Octroyer un accès aux CMK en vue de leur utilisation avec les AMI chiffrées et les instantanés EBS

Si vous spécifiez une [AMI chiffrée](#) ou un instantané Amazon EBS chiffré dans votre demande Spot Fleet et que vous utilisez une clé gérée par le client pour le chiffrement, vous devez accorder au `AWSServiceRoleForEC2SpotFleet` rôle l'autorisation d'utiliser le CMK afin qu'Amazon EC2 puisse lancer des instances en votre nom. Pour cela, vous devez ajouter une autorisation à la CMK, comme indiqué dans la procédure suivante.

Lorsque vous définissez les autorisations, les octrois constituent une alternative aux politiques de clé. Pour plus d'informations, consultez [Utilisation des octrois](#) et [Utilisation des stratégies de clé dans AWS KMS](#) dans le Guide du développeur AWS Key Management Service .

Pour accorder au `AWSServiceRoleForEC2SpotFleet` rôle l'autorisation d'utiliser le CMK

- Utilisez la commande [create-grant](#) pour ajouter une autorisation au CMK et pour spécifier le principal (le rôle `AWSServiceRoleForEC2SpotFleet` lié au service) autorisé à effectuer les opérations autorisées par l'autorisation. La CMK est spécifiée par le paramètre `key-id` et l'ARN de la CMK. Le principal est spécifié par le `grantee-principal` paramètre et l'ARN du rôle `AWSServiceRoleForEC2SpotFleet` lié au service.

```
aws kms create-grant \  
  --region us-east-1 \  
  --key-id arn:aws:kms:us-east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \  
  --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2SpotFleet \  
  --operations "Decrypt" "Encrypt" "GenerateDataKey" "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom" "ReEncryptTo"
```

Rôle lié à un service pour les instances Spot

Amazon EC2 utilise le rôle lié au service nommé `AWSServiceRoleForEC2Spot` pour lancer et gérer les instances Spot en votre nom. Pour plus d'informations, consultez [Rôle lié à un service pour les demandes d'instance Spot](#).

Rôle IAM pour l'étiquetage d'un parc d'instances Spot

Le rôle IAM `aws-ec2-spot-fleet-tagging-role` accorde au parc d'instances Spot l'autorisation d'étiqueter la demande, les instances et les volumes. Pour plus d'informations, consultez [Étiqueter un parc d'instances Spot](#).

Important

Si vous choisissez d'étiqueter des instances dans la flotte et que vous choisissez également de maintenir la capacité cible (la demande de parc d'instances Spot est de type `maintain`), les différences dans les autorisations qui sont définies pour l'utilisateur et le rôle `IamFleetRole` peuvent entraîner un comportement d'étiquetage incohérent pour les instances de la flotte. Si le rôle `IamFleetRole` n'inclut pas l'autorisation `CreateTags`, il se peut que certaines instances lancées par le parc ne soient pas balisées. En attendant que cette incohérence soit corrigée, pour vous assurer que toutes les instances lancées par le parc sont marquées, nous vous recommandons d'utiliser le rôle `aws-ec2-spot-fleet-tagging-role` pour `IamFleetRole`. Sinon, pour utiliser un rôle existant, associez la politique `AmazonEC2SpotFleetTaggingRole` AWS gérée au rôle existant. Sinon, vous devrez ajouter manuellement l'autorisation `CreateTags` à votre stratégie.

Pour créer le rôle IAM pour l'étiquetage d'un parc d'instances Spot

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Rôles.
3. Sélectionnez `Create role` (Créer un rôle).
4. Sur la page `Select trusted entity` (Sélectionner entité de confiance), sous `Trusted entity type` (Type d'entité de service) choisissez `AWS service`.
5. Sous `Cas d'utilisation`, dans `Cas d'utilisation pour d'autres AWS services`, choisissez `EC2`, puis `EC2 - Spot Fleet Tagging`.
6. Choisissez `Suivant`.

7. Sur la page Add permissions (Ajouter des autorisations), sélectionnez Next (Suivant).
8. Sur la page Name, review, and create (Nommer, réviser et créer) pour le Role name (nom de rôle), saisissez un nom de rôle (par exemple **aws-ec2-spot-fleet-tagging-role**).
9. Vérifiez les informations sur la page, puis choisissez Create role(Créer un rôle).

Prévention du cas de figure de l'adjoint désorienté entre services

Le [problème de l'adjoint confus](#) est un problème de sécurité dans lequel une entité qui n'a pas l'autorisation d'effectuer une action peut contraindre une entité plus privilégiée à effectuer cette action. Nous vous recommandons d'utiliser les clés de contexte de condition globale [aws:SourceArn](#) et [aws:SourceAccount](#) dans la politique d'approbation `aws-ec2-spot-fleet-tagging-role` pour limiter les autorisations que le parc d'instances Spot octroie à un autre service pour la ressource.

Pour ajouter les clés de SourceAccount condition `aws : SourceArn` et `aws :` à la politique de **aws-ec2-spot-fleet-tagging-role** confiance

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, sélectionnez Rôles.
3. Recherchez la valeur `aws-ec2-spot-fleet-tagging-role` que vous avez créé précédemment et sélectionnez le lien (et non la case à cocher).
4. Sous Summary Summary (Résumé), sélectionnez l'onglet Trust relationships (Relations d'approbation), puis Edit trust policy (Modifier la politique d'approbation).
5. Dans l'instruction JSON, ajoutez un `Condition` élément contenant votre `aws:SourceAccount` et `aws:SourceArn` Clés de contexte de condition globales pour empêcher le [problème de l'adjoint confus](#), comme suit :

```
"Condition": {
  "ArnLike": {
    "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
  },
  "StringEquals": {
    "aws:SourceAccount": "account_id"
  }
}
```

Note

Si vous utilisez les deux clés de contexte de condition globale et que la valeur de `aws:SourceArn` contient l'ID de compte, la valeur de `aws:SourceAccount` et le compte indiqué dans la valeur de `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'il est utilisé dans la même déclaration de politique.

La stratégie d'approbation finale sera la suivante :

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
    }
  }
}
```

6. Choisissez Mettre à jour une politique.

Le tableau suivant fournit les valeurs potentielles pour `aws:SourceArn` pour limiter la portée de votre `aws-ec2-spot-fleet-tagging-role` à divers degrés de spécificité.

Opération API	Service appelé	Portée	aws:SourceArn
RequestSpotFlotte	AWS STS (AssumeRole)	Limitez la AssumeRole aws-ec2-spot-fleet-tagging-role capacité spot-fleet-requests au compte spécifié.	arn:aws:ec2:*: 123456789012 :spot-fleet-request/sfr-*
RequestSpotFlotte	AWS STS (AssumeRole)	Limitez la AssumeRole capacité aws-ec2-spot-fleet-tagging-role spot-fleet-requests au compte et à la région spécifiés . Notez que ce rôle ne sera pas utilisable dans d'autres régions.	arn:aws:ec2: us-east-1 : 123456789012 :spot-fleet-request/sfr-*
RequestSpotFlotte	AWS STS (AssumeRole)	Limitez la AssumeRole capacité suraws-ec2-spot-fleet-tagging-role uniquement aux actions affectant la flotte sfr-11111111-1111-1111-1111-1111-111111111111. Notez que ce rôle peut ne pas être utilisable pour d'autres f Spot Fleets. De plus, ce rôle ne peut pas être utilisé pour lancer de nouvelles Spot Fleets	arn:aws:ec2: us-east-1 : 123456789012 :spot-fleet-request/sfr- 11111111-1111-1111-1111-11111111

Opération API	Service appelé	Portée	aws:SourceArn
		via Request-Spot-Fleet.	

Créer une Spot Fleet request

À l'aide du AWS Management Console, créez rapidement une demande Spot Fleet en choisissant uniquement les besoins de votre application ou de votre tâche et les spécifications de calcul minimales. Amazon EC2 configure une flotte qui répond le mieux à vos besoins et qui est conforme aux bonnes pratiques en matière d'instances Spot. Pour plus d'informations, consultez [Création rapide d'une demande de parc d'instances Spot \(console\)](#). Sinon, vous pouvez modifier l'un des paramètres par défaut. Pour plus d'informations, consultez [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#) et [Créez une flotte de spots à l'aide du AWS CLI](#).

Options de création d'un parc d'instances Spot

- [Création rapide d'une demande de parc d'instances Spot \(console\)](#)
- [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#)
- [Créez une flotte de spots à l'aide du AWS CLI](#)

Création rapide d'une demande de parc d'instances Spot (console)

Pour créer rapidement une demande de parc d'instances Spot , procédez comme suit.

Pour créer une demande de parc d'instances Spot à l'aide des paramètres recommandés (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Si vous utilisez les instances Spot pour la première fois, sélectionnez Mise en route. Sinon, sélectionnez Demander des Instances Spot.
4. Sous Launch parameters (Paramètres de lancement), choisissez Manually configure launch parameters (Configuration manuelle des paramètres de lancement).
5. Pour AMI, choisissez une AMI.

6. Sous Target capacity (Capacité cible), pour Total target capacity (Capacité cible totale), indiquez le nombre d'unités à demander. Pour le type d'unité, vous pouvez choisir Instances, vCPU ou Memory (MiB) (Mémoire (MiB)).
7. Pour Your fleet request at a glance (Votre demande de flotte en un coup d'œil), passez en revue la configuration de votre flotte et choisissez Launch (Lancer).

Création d'une demande de parc d'instances Spot à l'aide des paramètres définis (console)

Vous pouvez créer un parc d'instances Spot à l'aide des paramètres que vous définissez.

Pour créer une demande de parc d'instances Spot à l'aide des paramètres définis (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Si vous utilisez les instances Spot pour la première fois, sélectionnez Mise en route. Sinon, sélectionnez Demander des Instances Spot.
4. Pour Launch parameters (Paramètres de lancement), procédez comme suit :
 - a. Pour définir les paramètres de lancement dans la console Spot, choisissez Manually configure launch parameters (Configuration manuelle des paramètres de lancement).
 - b. Pour l'AMI, choisissez l'une des AMI de base fournies par AWS, ou choisissez Rechercher une AMI pour utiliser une AMI de notre communauté d'utilisateurs AWS Marketplace, ou l'une des vôtres.

 Note

Si une AMI spécifiée dans les paramètres de lancement est désenregistrée ou désactivée, aucune nouvelle instance ne peut être lancée à partir de l'AMI. Pour les flottes conçues pour maintenir la capacité cible, la capacité cible ne sera pas maintenue.

- c. (Facultatif) Pour Nom de la paire de clés, choisissez une paire de clés existante ou créez-en une.

[Paire de clés existante] Choisissez la paire de clés.

[Nouvelle paire de clés] Choisissez Create new key pair (Créer une nouvelle paire de clés) pour accéder à la page Key Pairs (Paires de clés). Lorsque vous avez terminé, revenez à la page Spot Requests (Demandes Spot) puis actualisez la liste.

- d. (Facultatif) Développez Additional launch parameters (Paramètres de lancement supplémentaires) et procédez comme suit.
 - i. (Facultatif) Pour activer l'optimisation Amazon EBS, choisissez Launch EBS-optimized instances (Lancer les instances optimisées pour EBS) pour EBS-optimized (Optimisé pour EBS).
 - ii. (Facultatif) Pour ajouter de l'espace de stockage temporaire de niveau bloc pour vos instances, choisissez Attach at launch (Attacher au lancement) pour Stockage d'instance.
 - iii. (Facultatif) Pour ajouter de l'espace de stockage supplémentaire, sélectionnez Add new volume (Ajouter un nouveau volume), puis spécifiez des volumes de stockage d'instances ou des volumes Amazon EBS supplémentaires, selon le type d'instance.
 - iv. (Facultatif) Par défaut, la surveillance basique est activée pour vos instances. Pour activer la surveillance détaillée, pour Surveillance, sélectionnez Activer la surveillance CloudWatch détaillée.
 - v. (Facultatif) Pour exécuter une instance Spot dédiée, pour Location, choisissez Dédié : exécuter une instance dédiée.
 - vi. (Facultatif) Pour Groupes de sécurité, choisissez un ou plusieurs groupes de sécurité ou créez-en un.

[Groupe de sécurité existant] Choisissez un ou plusieurs groupes de sécurité.

[Nouveau groupe de sécurité] Choisissez Create new security group (Créer un nouveau groupe de sécurité) pour accéder à la page Security Groups (Groupes de sécurité). Lorsque vous avez terminé, revenez à Spot Requests (Demandes Spot), puis actualisez la liste.

- vii. (Facultatif) Pour rendre vos instances accessibles depuis Internet, choisissez Activer pour Auto-assign IPv4 Public IP (Attribuer automatiquement une adresse IP publique IPv4).
- viii. (Facultatif) Pour lancer vos Instances Spot avec un rôle IAM, pour IAM instance profile (Profil d'instance IAM), choisissez le rôle.
- ix. (Facultatif) Pour exécuter un script de démarrage, copiez-le dans Données utilisateur.

- x. (Facultatif) Pour ajouter une identification, choisissez Create tag (Créer une identification) et saisissez la clé et la valeur de l'identification, puis sélectionnez Create (Créer). Répétez l'opération pour chaque étiquette.

Pour chaque identification, pour étiqueter les instances et la demande de parc d'instances Spot avec la même identification, assurez-vous que Instances et Fleet (Flotte) sont sélectionnées. Pour étiqueter uniquement les instances lancées par la flotte, supprimer Fleet (Flotte). Pour étiqueter uniquement la demande de parc d'instances Spot, supprimez Instances.

5. Pour Additional request details (Détails de la demande supplémentaire), procédez comme suit :
 - a. Vérifiez les détails de la demande supplémentaire. Pour effectuer des modifications, décochez la case Apply defaults (Appliquer les valeurs par défaut).
 - b. (Facultatif) Pour IAM fleet role (Rôle de parc IAM), vous pouvez utiliser le rôle par défaut ou choisir un autre rôle. Choisissez Use default role (Utiliser le rôle par défaut) pour utiliser le rôle par défaut après avoir changé de rôle.
 - c. (Facultatif) Pour Prix maximum, vous pouvez utiliser le prix maximum par défaut (prix à la demande) ou indiquer le prix maximum que vous êtes prêt à payer. Vos instances Spot ne sont pas lancées si votre prix maximal est inférieur au prix spot pour les types d'instance que vous avez sélectionnés.
 - d. (Facultatif) Pour créer une demande valide uniquement pendant une période spécifique, modifiez les valeurs des champs Demande valide du et Demande valide jusqu'au.
 - e. (Facultatif) Par défaut, nous résilions vos instances Spot à l'expiration de la demande de parc d'instances Spot. Si vous souhaitez qu'elles continuent de s'exécuter après l'expiration de votre demande, décochez la case Terminate the instances when the request expires (Résilier les instances lorsque la demande expire).
 - f. (Facultatif) Pour enregistrer vos Instances Spot auprès d'un équilibreur de charge, choisissez Receive traffic from one or more load balancers (Recevoir le trafic d'un ou plusieurs équilibreurs de charge) et choisissez un ou plusieurs Equilibreurs de charge classiques ou groupes cibles.
6. Pour Minimum compute unit (Unité de calcul minimale), choisissez les spécifications matérielles minimales (vCPU, mémoire et stockage) dont vous avez besoin pour votre application ou votre tâche, as specs (en tant que spécifications) ou as an instance type (en tant que type d'instance).
 - Pour as specs (en tant que spécifications), indiquez le nombre de vCPU requis et la quantité de mémoire requise.

- Pour `as an instance type` (en tant que type d'instance), acceptez le type d'instance par défaut ou choisissez `Change the instance type` pour choisir un autre type d'instance.
7. Dans `Target capacity` (Capacité cible), effectuez les opérations suivantes :
- a. Pour `Total target capacity` (Capacité cible totale), indiquez le nombre d'unités à demander. Pour le type d'unité, vous pouvez choisir `Instances`, `vCPU` ou `Memory (MiB)` (Mémoire (MiB)). Pour spécifier une capacité cible de 0 afin d'ajouter une capacité ultérieurement, choisissez `Maintain target capacity` (Maintenir la capacité cible).
 - b. (Facultatif) Pour `Include On-Demand base capacity` (Inclure la capacité de base à la demande), indiquez le nombre d'unités à la demande à demander. Ce nombre doit être inférieur à la valeur du champ `Capacité cible totale`. Amazon EC2 calcule la différence et l'alloue aux unités `Spot` à demander.

 Important

Pour spécifier une capacité à la demande facultative, vous devez commencer par choisir un modèle de lancement.

- c. (Facultatif) Par défaut, Amazon EC2 met fin aux instances `Spot` lorsqu'elles sont interrompues. Pour maintenir la capacité cible, sélectionnez `Maintain target capacity` (Maintenir la capacité cible). Vous pouvez ensuite spécifier qu'Amazon EC2 met fin, arrête ou met en veille prolongée les instances `Spot` lorsqu'elles sont interrompues. Pour ce faire, choisissez l'option correspondante à partir de `Interruption behavior` (Comportement d'interruption).

 Note

Si une AMI spécifiée dans les paramètres de lancement est désenregistrée ou désactivée, aucune nouvelle instance ne peut être lancée à partir de l'AMI. Pour les flottes conçues pour maintenir la capacité cible, la capacité cible ne sera pas maintenue.

- d. (Facultatif) Pour autoriser le parc d'instances `Spot` à lancer une instance `Spot` de remplacement lorsqu'une notification de rééquilibrage d'instance est émise pour une instance `Spot` existante dans la flotte, sélectionnez `Capacity rebalance` (Rééquilibrage de capacité), puis sélectionnez une stratégie de remplacement d'instance. Si vous choisissez `Launch before terminate` (Lancer avant la résiliation), spécifiez le délai (en secondes) avant

que le parc d'instances Spot ne résilie les anciennes instances. Pour plus d'informations, consultez [Rééquilibrage de la capacité](#).

- e. (Facultatif) Pour contrôler le montant que vous payez par heure pour l'ensemble des instances Spot de votre flotte, sélectionnez Set maximum cost for Spot instances (Définir le coût maximum pour les instances Spot), puis saisissez le montant total maximal que vous êtes prêt à payer par heure. Une fois le prix total maximum atteint, le parc d'instances Spot arrête de lancer des instances Spot même si la capacité cible n'a pas été atteinte. Pour plus d'informations, consultez [Contrôle des dépenses](#).
8. Pour Network (Réseau), procédez comme suit :
- a. Pour Réseau, choisissez un VPC existant ou créez-en un.

[VPC existant] Choisissez le VPC.

[Nouveau VPC] Choisissez Créer un nouveau VPC pour accéder à la console Amazon VPC. Lorsque vous avez terminé, revenez dans l'assistant et actualisez la liste.
 - b. (Facultatif) Pour Zone de disponibilité, laissez AWS choisir les zones de disponibilité de vos Instances Spot ou indiquez une ou plusieurs zones de disponibilité.

Si vous avez plusieurs sous-réseaux dans une zone de disponibilité, choisissez le sous-réseau approprié dans Sous-réseau. Pour ajouter des sous-réseaux, choisissez Créer un nouveau sous-réseau pour accéder à la console Amazon VPC. Lorsque vous avez terminé, revenez dans l'assistant et actualisez la liste.
9. Pour Instance type requirements (Exigences de type d'instance), vous pouvez soit spécifier les attributs d'instance et laisser Amazon EC2 identifier les types d'instance optimaux avec ces attributs, soit spécifier une liste des instances. Pour plus d'informations, consultez [Sélection de type d'instance basée sur des attributs pour un parc d'instances Spot](#).
- a. Si vous choisissez Specify instance attributes that match your compute requirements (Spécifier les attributs d'instance qui correspondent à vos exigences de calcul), spécifiez les attributs de votre instance comme suit :
 - i. Pour vCPU, saisissez les nombres minimum et maximum de vCPU souhaités. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.

- ii. Pour Memory (GiB) (Mémoire (Gio)), saisissez la quantité minimale et maximale de mémoire souhaitée. Pour ne spécifier aucune limite, sélectionnez No minimum (Pas de minimum), No maximum (Pas de maximum), ou les deux.
 - iii. (Facultatif) Pour Additional instance attributes (Attributs d'instance supplémentaires), vous pouvez éventuellement spécifier un ou plusieurs attributs pour exprimer vos exigences de calcul plus en détail. Chaque attribut supplémentaire ajoute une contrainte supplémentaire à votre demande. Vous pouvez omettre les attributs supplémentaires. Lorsque ces attributs sont omis, les valeurs par défaut sont utilisées. Pour obtenir une description de chaque attribut et de leurs valeurs par défaut, consultez [get-spot-placement-scores](#) dans la Référence des commandes en ligne d'Amazon EC2.
 - iv. (Facultatif) Pour afficher les types d'instance avec vos attributs spécifiés, développez Preview matching instance types (Aperçu des types d'instance correspondants). Pour empêcher des types d'instances d'être utilisés dans votre demande, sélectionnez les instances, puis choisissez Exclude selected instance types (Exclure les types d'instances sélectionnés).
- b. Si vous choisissez Manually select instance types (Sélection manuelle des types d'instances), le parc d'instances Spot fournit une liste par défaut des types d'instances. Pour sélectionner d'autres types d'instances, choisissez Add instance types (Ajouter des types d'instances), sélectionnez les types d'instances à utiliser dans votre demande, puis choisissez Select (Sélectionner). Pour supprimer des types d'instance, sélectionnez les types d'instance et choisissez Delete (Supprimer).
10. Pour Allocation strategy (Stratégie d'allocation), choisissez la stratégie qui répond à vos besoins. Pour plus d'informations, consultez [Stratégies d'allocation pour instances Spot](#).
 11. Pour Your fleet request at a glance (Votre demande de flotte en un coup d'œil), passez en revue la configuration de votre flotte et effectuez les ajustements nécessaires.
 12. (Facultatif) Pour télécharger une copie de la configuration de lancement à utiliser avec le AWS CLI, choisissez JSON config.
 13. Choisissez Launch.

Le type de demande de parc d'instances Spot est `fleet`. Une fois la demande exécutée, les demandes de type `instance` sont ajoutées, avec l'état `active` et le statut `fulfilled`.

Créez une flotte de spots à l'aide du AWS CLI

Pour créer une demande Spot Fleet à l'aide du AWS CLI

- Utilisez la commande [request-spot-fleet](#) pour créer une demande de parc d'instances Spot.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Pour accéder à des exemples de fichiers de configuration, consultez [Exemples de configuration d'un parc d'instances Spot](#).

Voici un exemple de sortie :

```
{
  "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Étiqueter un parc d'instances Spot

Pour vous aider à classer et à gérer vos demandes de parc d'instances Spot , vous pouvez les étiqueter avec des métadonnées personnalisées. Vous pouvez affecter une étiquette à une demande de parc d'instances Spot lorsque vous la créez, ou après. Vous pouvez attribuer des balises à l'aide de la console Amazon EC2 ou d'un outil de ligne de commande.

Lorsque vous étiquetez une demande de parc d'instances Spot , les instances et les volumes lancés par le parc d'instances Spot ne sont pas étiquetés automatiquement. Vous devez étiqueter explicitement les instances et les volumes lancés par le parc d'instances Spot . Vous pouvez choisir d'affecter des étiquettes uniquement à la demande de parc d'instances Spot , ou uniquement aux instances lancées par la flotte, ou uniquement aux volumes attachés aux instances lancées par la flotte, ou aux trois.

Note

Les balises de volume ne sont prises en charge que pour les volumes attachés à instances à la demande. Vous ne pouvez pas baliser les volumes attachés à instances Spot.

Pour plus d'informations sur le fonctionnement des balises, consultez [Baliser vos ressources Amazon EC2](#).

Table des matières

- [Prérequis](#)
- [Étiqueter un nouveau parc d'instances Spot](#)
- [Étiqueter un nouveau parc d'instances Spot et les instances et volumes qu'il lance](#)
- [Étiqueter un parc d'instances Spot existant](#)
- [Affichez les étiquettes de demande de parc d'instances Spot](#)

Prérequis

Octroyez à l'utilisateur l'autorisation de baliser les ressources. Pour plus d'informations, consultez [Exemple : Baliser des ressources](#).

Pour accorder à un utilisateur l'autorisation de baliser les ressources

Créez une politique IAM qui inclut les éléments suivants :

- L'action `ec2:CreateTags`. Celle-ci accorde à l'utilisateur l'autorisation de créer des balises.
- L'action `ec2:RequestSpotFleet`. Celle-ci accorde à l'utilisateur l'autorisation de créer une demande de parc d'instances Spot.
- Pour `Resource`, vous devez spécifier `"*"`. Cela permet aux utilisateurs de baliser tous les types de ressources.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "TagSpotFleetRequest",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
      ],
      "Resource": "*"
    }
  ]
}
```

⚠ Important

Actuellement, nous ne prenons pas en charge les autorisations de niveau ressource pour la ressource `spot-fleet-request`. Si vous spécifiez `spot-fleet-request` en tant que ressource, vous recevrez une exception de non-autorisation lorsque vous tenterez de baliser le parc. L'exemple suivant illustre comment ne pas définir la stratégie.

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateTags",
    "ec2:RequestSpotFleet"
  ],
  "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Étiqueter un nouveau parc d'instances Spot

Pour étiqueter une nouvelle demande de parc d'instances Spot à l'aide de la console

1. Suivez la procédure [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#).
2. Pour ajouter une balise, développez Additional configurations (Configurations supplémentaires), choisissez Add new tag (Ajouter une nouvelle balise), puis entrez la clé et la valeur de la balise. Répétez l'opération pour chaque balise.

Pour chaque étiquette, vous pouvez étiqueter la demande de parc d'instances Spot et les instances avec la même étiquette. Pour baliser les deux, assurez-vous que les balises d'instance et les balises de parc sont sélectionnées. Pour étiqueter uniquement la demande de parc d'instances Spot, désactivez les étiquettes d'instance. Pour balisées uniquement les instances lancées par le parc, désactivez les balises de parc.

3. Remplissez les champs requis pour créer une demande de parc d'instances Spot, puis choisissez Lancer. Pour plus d'informations, consultez [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#).

Pour étiqueter une nouvelle demande Spot Fleet à l'aide du AWS CLI

Pour étiqueter une demande de parc d'instances Spot lors de sa création, configurez la demande de parc d'instances Spot comme suit :

- Spécifiez les étiquettes pour la demande de parc d'instances Spot dans SpotFleetRequestConfig.
- Pour ResourceType, spécifiez spot-fleet-request. Si vous indiquez une autre valeur, la demande de flotte échouera.
- Pour Tags, spécifiez la paire clé-valeur. Vous pouvez définir plusieurs paires clé-valeur.

Dans l'exemple suivant, la demande de parc d'instances Spot est étiquetée par deux étiquettes : Key=Environment et Value=Production, ainsi que Key=Cost-Center et Value=123.

```
{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
```

```
"IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
"LaunchSpecifications": [
  {
    "ImageId": "ami-0123456789EXAMPLE",
    "InstanceType": "c4.large"
  }
],
"SpotPrice": "5",
"TargetCapacity": 2,
"TerminateInstancesWithExpiration": true,
"Type": "maintain",
"ReplaceUnhealthyInstances": true,
"InstanceInterruptionBehavior": "terminate",
"InstancePoolsToUseCount": 1,
"TagSpecifications": [
  {
    "ResourceType": "spot-fleet-request",
    "Tags": [
      {
        "Key": "Environment",
        "Value": "Production"
      },
      {
        "Key": "Cost-Center",
        "Value": "123"
      }
    ]
  }
]
}
}
```

Étiqueter un nouveau parc d'instances Spot et les instances et volumes qu'il lance

Pour étiqueter une nouvelle demande Spot Fleet ainsi que les instances et volumes qu'elle lance à l'aide du AWS CLI

Pour étiqueter une demande de parc d'instances Spot lors de sa création et pour étiqueter les instances et les volumes lorsqu'ils sont lancés par la flotte, configurez la demande de parc d'instances Spot comme suit :

Étiquettes de demande de parc d'instances Spot

- Spécifiez les étiquettes pour la demande de parc d'instances Spot dans `SpotFleetRequestConfig`.
- Pour `ResourceType`, spécifiez `spot-fleet-request`. Si vous indiquez une autre valeur, la demande de flotte échouera.
- Pour `Tags`, spécifiez la paire clé-valeur. Vous pouvez définir plusieurs paires clé-valeur.

Balises d'instance :

- Spécifiez les balises des instances dans `LaunchSpecifications`.
- Pour `ResourceType`, spécifiez `instance`. Si vous indiquez une autre valeur, la demande de flotte échouera.
- Pour `Tags`, spécifiez la paire clé-valeur. Vous pouvez définir plusieurs paires clé-valeur.

Vous pouvez également spécifier les étiquettes de l'instance dans le [modèle de lancement](#) référencé dans la demande de parc d'instances Spot.

Balises de volume :

- Spécifiez les étiquettes des volumes dans le [modèle de lancement](#) référencé dans la demande de parc d'instances Spot. Le balisage de volume dans `LaunchSpecifications` n'est pas pris en charge.

Dans l'exemple suivant, la demande de parc d'instances Spot est étiquetée par deux étiquettes : `Key=Environment` et `Value=Production`, ainsi que `Key=Cost-Center` et `Value=123`. Les instances qui sont lancées par la flotte sont identifiées avec une étiquette (qui est la même que l'une des étiquettes de la demande de parc d'instances Spot) : `Key=Cost-Center` et `Value=123`.

```
{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchSpecifications": [
      {
        "ImageId": "ami-0123456789EXAMPLE",
```

```
        "InstanceType": "c4.large",
        "TagSpecifications": [
            {
                "ResourceType": "instance",
                "Tags": [
                    {
                        "Key": "Cost-Center",
                        "Value": "123"
                    }
                ]
            }
        ]
    },
    "SpotPrice": "5",
    "TargetCapacity": 2,
    "TerminateInstancesWithExpiration": true,
    "Type": "maintain",
    "ReplaceUnhealthyInstances": true,
    "InstanceInterruptionBehavior": "terminate",
    "InstancePoolsToUseCount": 1,
    "TagSpecifications": [
        {
            "ResourceType": "spot-fleet-request",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Cost-Center",
                    "Value": "123"
                }
            ]
        }
    ]
}
```

Pour étiqueter les instances lancées par un parc de spots à l'aide du AWS CLI

Pour étiqueter les instances lorsqu'elles sont lancées par la flotte, vous pouvez spécifier les étiquettes dans le [modèle de lancement](#) référencé dans la demande de parc d'instances Spot ou dans la configuration de la demande de parc d'instances Spot comme suit :

- Spécifiez les balises des instances dans `LaunchSpecifications`.
- Pour `ResourceType`, spécifiez `instance`. Si vous indiquez une autre valeur, la demande de flotte échouera.
- Pour `Tags`, spécifiez la paire clé-valeur. Vous pouvez définir plusieurs paires clé-valeur.

Dans l'exemple suivant, les instances lancées par la flotte sont marquées avec une balise : `Key=Cost-Center` et `Value=123`.

```
{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchSpecifications": [
      {
        "ImageId": "ami-0123456789EXAMPLE",
        "InstanceType": "c4.large",
        "TagSpecifications": [
          {
            "ResourceType": "instance",
            "Tags": [
              {
                "Key": "Cost-Center",
                "Value": "123"
              }
            ]
          }
        ]
      }
    ],
    "SpotPrice": "5",
    "TargetCapacity": 2,
    "TerminateInstancesWithExpiration": true,
    "Type": "maintain",
    "ReplaceUnhealthyInstances": true,
    "InstanceInterruptionBehavior": "terminate",
```

```
    "InstancePoolsToUseCount": 1
  }
}
```

Pour étiqueter les volumes attachés à des instances à la demande lancées par un parc d'instances Spot en utilisant la AWS CLI

Pour étiqueter des volumes lorsqu'ils sont créés par la flotte, spécifiez les étiquettes dans le [modèle de lancement](#) référencé dans la demande de parc d'instances Spot.

Note

Les balises de volume ne sont prises en charge que pour les volumes attachés à instances à la demande. Vous ne pouvez pas baliser les volumes attachés à instances Spot. Le balisage de volume dans `LaunchSpecifications` n'est pas pris en charge.

Étiqueter un parc d'instances Spot existant

Pour étiqueter une demande de parc d'instances Spot existante à l'aide de la console

Après avoir créé une demande de parc d'instances Spot , vous pouvez ajouter des étiquettes à la demande de flotte à l'aide de la console.

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez l'onglet Tags (Balises), puis Create Tag (Créer une balise).

Pour étiqueter une demande Spot Fleet existante à l'aide du AWS CLI

Utilisez la commande [create-tags](#) pour baliser les ressources existantes. Dans l'exemple suivant, la demande de parc d'instances Spot existante est étiquetée avec `Key=purpose` et `Value=test`.

```
aws ec2 create-tags \  
  --resources sfr-11112222-3333-4444-5555-6666EXAMPLE \  
  --tags Key=purpose,Value=test
```

Affichez les étiquettes de demande de parc d'instances Spot

Pour afficher les étiquettes d'une demande de parc d'instances Spot à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot et sélectionnez l'onglet Étiquette.

Pour décrire les étiquettes de demande de parc d'instances Spot

Utilisez la commande [describe-tags](#) pour afficher les balises de la ressource spécifiée. Dans l'exemple suivant, vous décrivez les étiquettes de la demande de parc d'instances Spot spécifiée.

```
aws ec2 describe-tags \  
  --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{  
  "Tags": [  
    {  
      "Key": "Environment",  
      "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",  
      "ResourceType": "spot-fleet-request",  
      "Value": "Production"  
    },  
    {  
      "Key": "Another key",  
      "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",  
      "ResourceType": "spot-fleet-request",  
      "Value": "Another value"  
    }  
  ]  
}
```

Vous pouvez également afficher les étiquettes d'une demande de parc d'instances Spot en décrivant la demande de parc d'instances Spot .

Utilisez la commande [describe-spot-fleet-requests](#) pour afficher la configuration de la demande de parc d'instances Spot spécifiée, qui inclut toutes les étiquettes définies pour la demande de flotte.

```
aws ec2 describe-spot-fleet-requests \  
  --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
--spot-fleet-request-ids sfr-11112222-3333-4444-5555-6666EXAMPLE
```

```
{
  "SpotFleetRequestConfigs": [
    {
      "ActivityStatus": "fulfilled",
      "CreateTime": "2020-02-13T02:49:19.709Z",
      "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "Default",
        "FulfilledCapacity": 2.0,
        "OnDemandFulfilledCapacity": 0.0,
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
        "LaunchSpecifications": [
          {
            "ImageId": "ami-0123456789EXAMPLE",
            "InstanceType": "c4.large"
          }
        ],
        "TargetCapacity": 2,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": false,
        "InstanceInterruptionBehavior": "terminate"
      },
      "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-6666EXAMPLE",
      "SpotFleetRequestState": "active",
      "Tags": [
        {
          "Key": "Environment",
          "Value": "Production"
        },
        {
          "Key": "Another key",
          "Value": "Another value"
        }
      ]
    }
  ]
}
```

Décrire votre parc d'instances Spot

Le parc d'instances Spot lance des instances Spot lorsque votre prix maximum dépasse le prix Spot et que la capacité est disponible. Les instances Spot s'exécutent jusqu'à ce qu'elles soient interrompues ou que vous les résilieez.

Pour décrire votre parc d'instances Spot (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot. Pour afficher les détails de la configuration, choisissez Description.
4. Pour répertorier les instances Spot du parc d'instances Spot, choisissez Instances.
5. Pour afficher l'historique du parc d'instances Spot, choisissez Historique.

Pour décrire votre parc d'instances Spot (AWS CLI)

Utilisez la commande [describe-spot-fleet-requests](#) pour décrire vos demandes de parc d'instances Spot.

```
aws ec2 describe-spot-fleet-requests
```

Utilisez la commande [describe-spot-fleet-instances](#) pour décrire les instances Spot du parc d'instances Spot spécifié.

```
aws ec2 describe-spot-fleet-instances \  
  --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Utilisez la commande [describe-spot-fleet-request-history](#) pour décrire l'historique de la demande de parc d'instances Spot spécifiée.

```
aws ec2 describe-spot-fleet-request-history \  
  --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \  
  --start-time 2015-05-18T00:00:00Z
```

Modifier une demande de parc d'instances Spot

Vous pouvez modifier une demande de parc d'instances Spot active pour effectuer les tâches suivantes :

- Augmenter la capacité cible et la partie à la demande
- Diminuer la capacité cible et la partie à la demande

Note

Vous ne pouvez pas modifier une demande unique de parc d'instances Spot . Vous pouvez uniquement modifier une demande de parc d'instances Spot si vous avez sélectionné Maintenir la capacité cible au moment de la création de la demande de parc d'instances Spot.

Lorsque vous augmentez la capacité cible, le parc d'instances Spot lance des instances Spot supplémentaires. Lorsque vous augmentez la part à la demande, le parc d'instances Spot lance des instances à la demande supplémentaires.

Lorsque vous augmentez la capacité cible, le parc d'instances ponctuelles lance les instances ponctuelles supplémentaires conformément à la [stratégie d'allocation](#) pour sa demande de parc d'instances ponctuelles.

Lorsque vous diminuez la capacité cible, le parc d'instances Spot annule les demandes ouvertes qui dépassent la nouvelle capacité cible. Vous pouvez demander à ce que le parc d'instances Spot résilie les instances Spot jusqu'à ce que la taille de la flotte atteigne la nouvelle capacité cible. Si la politique d'allocation sélectionnée est *diversified*, le parc d'instances Spot résilie les instances dans les groupes. Vous pouvez aussi demander à ce que le parc d'instances Spot conserve la taille actuelle de la flotte, mais sans remplacer les instances Spot interrompues ni les instances que vous résiliez manuellement.

Lorsqu'un parc d'instances Spot résilie une instance du fait de la diminution de la capacité cible, l'instance reçoit un avis d'interruption d'instance Spot.

Pour modifier une demande de parc d'instances Spot (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.

3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez Actions, Modify target capacity (Modifier la capacité cible).
5. Dans Modify target capacity (Modifier la capacité cible), effectuez les opérations suivantes :
 - a. Entrez la nouvelle capacité cible et la partie à la demande.
 - b. (Facultatif) Si vous diminuez la capacité cible, mais que vous souhaitez conserver la taille actuelle du parc, décochez la case Terminate instances (Résilier les instances).
 - c. Choisissez Submit.

Pour modifier une demande de parc Spot à l'aide du AWS CLI

Utilisez la commande [modify-spot-fleet-request](#) pour mettre à jour la capacité cible de la demande de parc d'instances Spot spécifiée.

```
aws ec2 modify-spot-fleet-request \  
  --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \  
  --target-capacity 20
```

Vous pouvez modifier la commande précédente comme suit de façon à diminuer la capacité cible de la flotte Spot spécifié sans que cela n'ait pour effet de résilier les instances Spot.

```
aws ec2 modify-spot-fleet-request \  
  --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \  
  --target-capacity 10 \  
  --excess-capacity-termination-policy NoTermination
```

Annulation d'une demande de parc d'instances Spot

Si vous n'avez plus besoin d'instances Spot, vous pouvez annuler la demande de parc d'instances Spot. Après l'annulation d'une demande de flotte, toutes les demandes Spot associées à la flotte sont également annulées, de sorte qu'aucune nouvelle instance Spot n'est lancée.

Lorsque vous annulez une demande de parc d'instances Spot, vous devez également spécifier si vous voulez résilier toutes ses instances. Cette action inclut les instances à la demande et les instances Spot.

Si vous spécifiez que les instances doivent être résiliées lorsque la demande de flotte est annulée, celle-ci entre dans l'état `cancelled_terminating`. Sinon, la demande de flotte passe à l'état

cancelled_running et les instances continuent à être exécutées jusqu'à ce qu'elles soient interrompues ou jusqu'à ce que vous les mettiez hors service manuellement.

Restrictions

- Vous pouvez supprimer jusqu'à 100 flottes en une seule demande. Si vous dépassez le nombre spécifié, aucune flotte n'est supprimée.

Pour annuler une demande de parc d'instances Spot (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot.
4. Choisissez Actions, Annuler la demande.
5. Dans la boîte de dialogue Annuler la demande de flotte, procédez comme suit :
 - a. Pour résilier les instances associées en même temps que vous annulez la demande de parc d'instances Spot, ne décochez pas la case Résilier les instances. Pour annuler la demande de parc d'instances Spot sans résilier les instances associées, décochez la case Résilier les instances.
 - b. Choisissez Confirmer.

Pour annuler une demande Spot Fleet et mettre fin à ses instances à l'aide du AWS CLI

Utilisez la commande [cancel-spot-fleet-requests](#) pour annuler la demande de parc d'instances Spot spécifiée et résilier ses instances à la demande et ses instances Spot.

```
aws ec2 cancel-spot-fleet-requests \  
  --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \  
  --terminate-instances
```

Exemple de sortie

```
{  
  "SuccessfulFleetRequests": [  
    {  
      "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",  
      "CurrentSpotFleetRequestState": "cancelled_terminating",
```

```
        "PreviousSpotFleetRequestState": "active"
    }
],
"UnsuccessfulFleetRequests": []
}
```

Pour annuler une demande de parc d'instances Spot sans résilier ses instances à l'aide de la commande AWS CLI

Vous pouvez modifier la commande précédente en utilisant le paramètre `--no-terminate-instances` pour annuler la demande de parc d'instances Spot spécifiée sans résilier ses instances à la demande et ses instances Spot.

```
aws ec2 cancel-spot-fleet-requests \
  --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
  --no-terminate-instances
```

Exemple de sortie

```
{
  "SuccessfulFleetRequests": [
    {
      "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
      "CurrentSpotFleetRequestState": "cancelled_running",
      "PreviousSpotFleetRequestState": "active"
    }
  ],
  "UnsuccessfulFleetRequests": []
}
```

CloudWatch métriques pour Spot Fleet

Amazon EC2 fournit des CloudWatch métriques Amazon que vous pouvez utiliser pour surveiller votre parc de spots.

Important

Pour garantir la précision des informations, nous vous recommandons d'activer la surveillance détaillée lorsque vous utilisez ces métriques. Pour plus d'informations, consultez [Activer ou désactiver la surveillance détaillée pour vos instances.](#)

Pour plus d'informations sur CloudWatch les métriques fournies par Amazon EC2, consultez.

[Surveillez vos instances à l'aide de CloudWatch](#)

Métriques du parc d'instances Spot

L'espace de AWS/EC2Spot noms inclut les métriques suivantes, ainsi que les CloudWatch métriques relatives aux instances Spot de votre flotte. Pour plus d'informations, consultez [Métriques des instances](#).

Métrique	Description
AvailableInstancePoolsCount	Les groupes de capacités Spot spécifiés dans la demande de parc d'instances Spot . Unités : nombre
BidsSubmittedForCapacity	Capacité pour laquelle Amazon EC2 a envoyé des demandes de parc d'instances Spot . Unités : nombre
EligibleInstancePoolCount	Groupes de capacités Spot spécifiés dans la demande de parc d'instances Spot où Amazon EC2 peut traiter les demandes. Amazon EC2 ne répond pas aux demandes dans les groupes où le prix maximum que vous acceptez de payer pour les instances Spot est inférieur au prix Spot ou lorsque le prix Spot est supérieur au prix des instances à la demande. Unités : nombre
FulfilledCapacity	Capacité exécutée par Amazon EC2. Unités : nombre
MaxPercentCapacityAllocation	

Métrique	Description
	<p>Valeur maximale de <code>PercentCapacityAllocation</code> pour tous les groupes de parc d'instances Spot spécifiés dans la demande de parc d'instances Spot.</p> <p>Unités : pourcentage</p>
<code>PendingCapacity</code>	<p>Différence entre <code>TargetCapacity</code> et <code>FulfilledCapacity</code>.</p> <p>Unités : nombre</p>
<code>PercentCapacityAllocation</code>	<p>Capacité allouée pour le groupe de capacités Spot pour les dimensions spécifiées. Pour obtenir la valeur maximale enregistrée sur tous les groupes de capacités Spot, utilisez <code>MaxPercentCapacityAllocation</code>.</p> <p>Unités : pourcentage</p>
<code>TargetCapacity</code>	<p>Capacité cible d'une demande de parc d'instances Spot.</p> <p>Unités : nombre</p>
<code>TerminatingCapacity</code>	<p>Capacité résiliée car la capacité allouée est supérieure à la capacité cible.</p> <p>Unités : nombre</p>

Si l'unité de mesure d'une métrique est `Count`, la statistique la plus utile est `Average`.

Dimensions du parc d'instances Spot

Pour filtrer les données de votre parc d'instances Spot, utilisez les dimensions suivantes.

Dimensions	Description
AvailabilityZone	Filtrer les données par Zone de disponibilité.
FleetRequestId	Filtrer les données demande de parc d'instances Spot.
InstanceType	Filtrer les données par type d'instance.

Consultez les CloudWatch statistiques de votre flotte Spot

Vous pouvez consulter les CloudWatch statistiques de votre parc de spots à l'aide de la CloudWatch console Amazon. Ces métriques s'affichent sous forme de graphiques de surveillance. Ces graphiques affichent des points de données si le parc d'instances Spot est actif.

Les métriques sont d'abord regroupées par espace de noms, puis par les différentes combinaisons de dimensions au sein de chaque espace de noms. Par exemple, vous pouvez afficher toutes les métriques du parc d'instances Spot ou les groupes de métriques du parc d'instances Spot par ID de demande de parc d'instances Spot, type d'instance ou zone de disponibilité.

Pour afficher les métriques du parc d'instances Spot

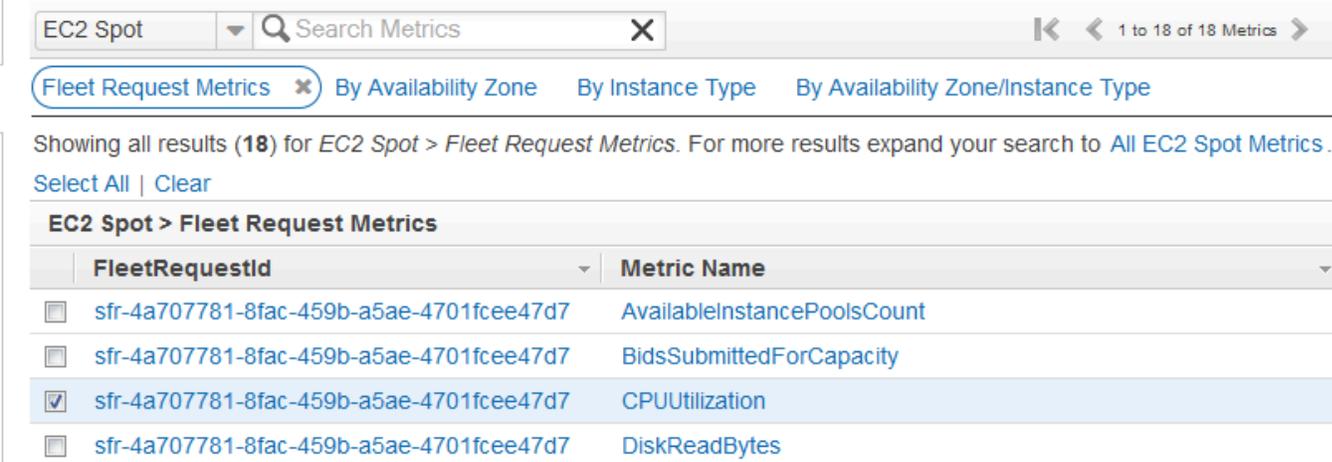
1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le volet de navigation, sélectionnez Metrics (Métriques).
3. Choisissez l'espace de noms EC2 Spot.

Note

Si l'espace de noms EC2 Spot n'est pas affiché, c'est pour deux raisons. Soit vous n'avez pas encore utilisé Spot Fleet. Seuls les AWS services que vous utilisez envoient des statistiques à Amazon. CloudWatch Soit, si vous n'avez pas utilisé le parc d'instances Spot au cours des deux dernières semaines, l'espace de noms n'apparaît pas.

4. (Facultatif) Pour filtrer les métriques par dimension, sélectionnez l'une des options suivantes :
 - Métriques de demande de parc : regroupement par demande de parc d'instances Spot

- Par zone de disponibilité : regroupement par demande de parc d'instances Spot et zone de disponibilité
 - Par type d'instance : regroupement par demande de parc d'instances Spot et type d'instance
 - Par zone de disponibilité/Type d'instance : regroupement par demande de parc d'instances Spot, zone de disponibilité et type d'instance
5. Pour afficher les données d'une métrique, cochez la case en regard de la métrique.



EC2 Spot Search Metrics 1 to 18 of 18 Metrics

Fleet Request Metrics By Availability Zone By Instance Type By Availability Zone/Instance Type

Showing all results (18) for EC2 Spot > Fleet Request Metrics. For more results expand your search to All EC2 Spot Metrics. Select All | Clear

EC2 Spot > Fleet Request Metrics

FleetRequestId	Metric Name
<input type="checkbox"/> sfr-4a707781-8fac-459b-a5ae-4701fcee47d7	AvailableInstancePoolsCount
<input type="checkbox"/> sfr-4a707781-8fac-459b-a5ae-4701fcee47d7	BidsSubmittedForCapacity
<input checked="" type="checkbox"/> sfr-4a707781-8fac-459b-a5ae-4701fcee47d7	CPUUtilization
<input type="checkbox"/> sfr-4a707781-8fac-459b-a5ae-4701fcee47d7	DiskReadBytes

Scalabilité automatique du parc d'instances Spot

La scalabilité automatique est l'aptitude à augmenter ou à diminuer automatiquement la capacité cible de votre parc d'instances Spot en fonction de la demande. Un parc d'instances Spot peut lancer des instances (augmenter) ou résilier des instances (diminuer), dans la plage que vous choisissez, en réponse à une ou plusieurs politiques de mise à l'échelle.

Le parc d'instances Spot prend en charge les types de scalabilité automatique suivants :

- [Mise à l'échelle du suivi de cible](#) : augmente ou réduit la capacité actuelle de la flotte en fonction d'une valeur cible pour une métrique spécifique. Cette option est similaire à la façon dont votre thermostat maintient la température de votre domicile : vous sélectionnez une température et le thermostat se charge du reste.
- [Mise à l'échelle d'étape](#) : augmente ou réduit la capacité actuelle de la flotte en fonction d'un ensemble d'ajustements de la mise à l'échelle, appelés ajustements d'étape, qui varient en fonction de la valeur d'utilisation hors limites de l'alarme.
- [Mise à l'échelle planifiée](#) : augmente ou réduit la capacité actuelle de la flotte en fonction de la date et de l'heure.

Si vous utilisez une [pondération d'instance](#), gardez à l'esprit que le parc d'instances Spot peut dépasser la capacité cible si nécessaire. La capacité fournie peut correspondre à un nombre à virgule flottante, mais la capacité cible doit être un nombre entier pour que le parc d'instances Spot puisse l'arrondir au nombre entier suivant. Vous devez prendre ces comportements en compte lorsque vous examinez les résultats d'une politique de dimensionnement lorsqu'une alarme se déclenche. Par exemple, supposons que la capacité cible est 30, que la capacité fournie est 30,1 et que la politique de dimensionnement soustrait 1. Lorsque l'alarme se déclenche, le processus de scalabilité automatique soustrait 1 de 30,1 pour obtenir 29,1, puis arrondit la valeur à 30. Aucune action de mise à l'échelle n'est alors effectuée. Pour prendre un autre exemple, supposons que vous avez sélectionné des pondérations d'instance de 2, 4 et 8, et une capacité cible de 10, mais qu'aucune instance de pondération 2 n'était disponible, si bien que le parc d'instances Spot a provisionné des instances de pondération 4 et 8 pour une capacité fournie de 12. Si la politique de mise à l'échelle réduit la capacité cible de 20 % et qu'une alarme se déclenche, le processus de scalabilité automatique soustrait $12 \times 0,2$ de 12 pour obtenir 9,6, puis arrondit la valeur à 10. Aucune action de mise à l'échelle n'est alors effectuée.

Les politiques de mise à l'échelle que vous créez pour le parc d'instances Spot prennent en charge un temps de stabilisation. C'est le nombre de secondes après la fin d'une activité de dimensionnement au cours desquelles les activités de dimensionnement précédentes liées à un déclencheur peuvent influencer sur les événements de dimensionnement futurs. Pour les politiques de montée en charge (scale-out), pendant la durée du temps de stabilisation, la capacité qui a été ajoutée par l'événement de montée en charge précédent qui a lancé la stabilisation est calculée dans le cadre de la capacité souhaitée pour la montée en charge suivante. L'objectif est d'effectuer une montée en charge continue (mais pas excessive). Pour les politiques de diminution de charge, la période de récupération est utilisée pour bloquer les demandes de montée en charge suivantes jusqu'à leur expiration. L'objectif est de diminuer la charge avec prudence afin de protéger la disponibilité de votre application. Toutefois, si une autre alarme déclenche une politique de montée en charge pendant le temps de stabilisation après une diminution en charge (scale-in), la scalabilité automatique monte immédiatement en charge votre cible scalable.

Nous vous recommandons de dimensionner sur des métriques d'instance à une fréquence de 1 minute, car cela permet de réagir plus rapidement aux modifications d'utilisation. Un dimensionnement sur des métriques à une fréquence de 5 minutes peut entraîner des temps de réponse plus lents et un dimensionnement sur des données de métrique obsolètes. Pour envoyer des données métriques pour vos instances par périodes d' CloudWatch une minute, vous devez spécifiquement activer la surveillance détaillée. Pour plus d'informations, consultez [Activer](#)

[ou désactiver la surveillance détaillée pour vos instances](#) et [Création d'une demande de parc d'instances Spot à l'aide des paramètres définis \(console\)](#).

Pour plus d'informations sur la configuration de la mise à l'échelle du parc d'instances Spot , consultez les ressources suivantes :

- Section [application-autoscaling](#) du document AWS CLI Référence des commandes
- [Référence de l'API Application Auto Scaling](#)
- [Guide de l'utilisateur Application Auto Scaling](#)

Autorisations IAM requises pour la scalabilité automatique d'un parc d'instances Spot

Le dimensionnement automatique pour Spot Fleet est rendu possible par une combinaison des API Amazon EC2 CloudWatch, Amazon et Application Auto Scaling. Les demandes Spot Fleet sont créées avec Amazon EC2, les alarmes sont créées avec CloudWatch Application Auto Scaling et les politiques de dimensionnement sont créées avec Application Auto Scaling.

Outre les [autorisations IAM pour le parc d'instances Spot](#), et Amazon EC2, l'utilisateur qui accède aux paramètres de mise à l'échelle de la flotte doit disposer des autorisations appropriées pour les services qui prennent en charge la mise à l'échelle dynamique. Les utilisateurs doivent être autorisés à utiliser les actions dans l'exemple de politique suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "application-autoscaling:*",
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
```

```
        "iam:CreateServiceLinkedRole",
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:Get*",
        "sns:List*"
    ],
    "Resource": "*"
}
]
```

Vous pouvez également créer vos propres politiques IAM qui permettent de créer des autorisations plus détaillées pour les appels vers l'API Application Auto Scaling. Pour plus d'informations, veuillez consulter [Authentification et contrôle d'accès](#) dans le Guide de l'utilisateur Application Auto Scaling.

Le service Application Auto Scaling a également besoin d'une autorisation pour décrire votre parc de spots et vos CloudWatch alarmes, ainsi que d'autorisations pour modifier la capacité cible de votre parc de spots en votre nom. Si vous activez la scalabilité automatique pour votre parc d'instances Spot, il crée un rôle lié à un service nommé `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest`. Le rôle lié à un service donne à Application Auto Scaling l'autorisation de décrire les alarmes de vos politiques, de surveiller la capacité actuelle du flotte et éventuellement de la modifier. Le rôle de parc d'instances Spot géré original pour Application Auto Scaling était `aws-ec2-spot-fleet-autoscale-role`, mais il n'est plus nécessaire. Le rôle lié à un service est le rôle par défaut pour Application Auto Scaling. Pour plus d'informations, consultez [Rôles liés à un service](#) dans le Guide de l'utilisateur Application Auto Scaling.

Mise à l'échelle d'un parc d'instances Spot en utilisant une politique de suivi de cible

Grâce aux politiques de suivi des objectifs et d'échelonnement, vous sélectionnez une métrique et définissez une valeur cible. Spot Fleet crée et gère les CloudWatch alarmes qui déclenchent la politique de dimensionnement et calcule l'ajustement de dimensionnement en fonction de la métrique et de la valeur cible. La politique de dimensionnement ajoute ou supprime de la capacité si nécessaire pour maintenir la métrique à la valeur cible spécifiée ou proche de celle-ci. En plus de maintenir la métrique proche de la valeur cible, une politique de dimensionnement Suivi de la cible s'ajuste également aux fluctuations de la métrique dues à un modèle de charge fluctuant, et minimise les fluctuations rapides dans la capacité du flotte.

Vous pouvez créer plusieurs politiques de suivi des objectifs et d'échelonnement pour un parc d'instances Spot dans la mesure où chacune d'elles utilise une métrique différente. Le flotte est

dimensionné selon la politique qui fournit la plus grande capacité de flotte. Cela vous permet de couvrir plusieurs scénarios et de toujours disposer d'une capacité suffisante pour traiter vos charges de travail d'application.

Pour garantir la disponibilité de l'application, la flotte augmente proportionnellement aux métriques aussi rapidement que possible, mais diminue plus progressivement.

Lorsqu'un parc d'instances Spot résilie une instance du fait de la diminution de la capacité cible, l'instance reçoit un avis d'interruption d'instance Spot.

Ne modifiez ni ne supprimez les CloudWatch alarmes gérées par Spot Fleet dans le cadre d'une politique de dimensionnement du suivi des cibles. Le parc d'instances Spot supprime les alarmes automatiquement lorsque vous supprimez la politique de suivi des objectifs et d'échelonnement.

Limitation

La demande de parc d'instances Spot doit être de type `maintain`. La scalabilité automatique n'est pas prise en charge pour les demandes de type `request`.

Pour configurer une politique de suivi de cible (console)

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot et choisissez Auto Scaling.
4. Si la mise à l'échelle automatique n'est pas configurée, sélectionnez Configurer.
5. Utilisez le champ Scale capacity between (Mettre à l'échelle la capacité entre) pour définir les capacités minimale et maximale de votre parc. Avec le dimensionnement automatique, votre flotte n'aura jamais une capacité inférieure ou supérieure aux limites fixées.
6. Pour Policy name (Nom de la stratégie), attribuez un nom à cette stratégie.
7. Choisissez une valeur Target Metric (Métrique cible).
8. Spécifiez une valeur Target Value (Valeur cible) pour la métrique.
9. Pour le Temps de stabilisation, spécifiez une nouvelle valeur (en secondes) ou conservez la valeur par défaut.
10. (Facultatif) Sélectionnez Disable Scale-in (Désactiver la diminution en charge) pour ignorer la création d'une stratégie de diminution en charge sur la base de la configuration en cours. Vous pouvez créer une politique d'ajustement à la baisse à l'aide d'une autre configuration.

11. Choisissez Enregistrer.

Pour configurer une politique de suivi des cibles à l'aide du AWS CLI

1. Enregistrez la demande de parc d'instances Spot en tant que cible évolutive à l'aide de la commande [register-scalable-target](#).
2. Créez une stratégie de mise à l'échelle à l'aide de la commande [put-scaling-policy](#).

Mise à l'échelle du parc d'instances Spot en utilisant les politiques de mise à l'échelle d'étape

Avec les politiques de dimensionnement par étapes, vous spécifiez CloudWatch des alarmes pour déclencher le processus de dimensionnement. Par exemple, si vous souhaitez augmenter la capacité du parc quand l'utilisation de l'UC atteint un niveau donné, créez une alarme en utilisant la métrique `CPUUtilization` fournie par Amazon EC2.

Lorsque vous créez une politique de dimensionnement d'étape, vous devez indiquer l'un des types d'ajustement suivants :

- Ajouter : augmentez la capacité cible de la flotte selon un nombre donné d'unités de capacité ou un pourcentage de la capacité actuelle spécifié.
- Supprimer : réduisez la capacité cible de la flotte selon un nombre donné d'unités de capacité ou un pourcentage de la capacité actuelle spécifié.
- Définir sur : définissez la capacité cible de la flotte selon un nombre précis d'unités de capacité spécifié.

Lorsqu'une alarme se déclenche, le processus de scalabilité automatique calcule la nouvelle capacité cible d'après la capacité fournie et la politique de mise à l'échelle, puis met à jour la capacité cible en conséquence. Par exemple, supposons que la capacité cible et la capacité fournie sont égales à 10 et que la politique de dimensionnement ajoute 1. Lorsque l'alarme se déclenche, le processus de scalabilité automatique ajoute 1 à 10 pour obtenir 11, pour que le parc d'instances Spot lance 1 instance.

Lorsqu'un parc d'instances Spot résilie une instance du fait de la diminution de la capacité cible, l'instance reçoit un avis d'interruption d'instance Spot.

Limitation

La demande de parc d'instances Spot doit être de type `maintain`. La mise à l'échelle automatique n'est pas pris en charge pour les demandes de type `request` et les blocs d'instances Spot.

Prérequis

- Déterminez quels CloudWatch indicateurs sont importants pour votre application. Vous pouvez créer des CloudWatch alarmes en fonction des métriques fournies par AWS ou de vos propres métriques personnalisées.
- Pour les AWS métriques que vous utiliserez dans vos politiques de dimensionnement, activez la collecte de CloudWatch métriques si le service qui fournit les métriques ne l'active pas par défaut.

Pour créer une CloudWatch alarme

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le panneau de navigation, cliquez sur Alarms (Alarmes).
3. Sélectionnez Créer une alarme.
4. Sur la page Specify metric and conditions (Spécifier une métrique et des conditions), sélectionnez Select metric (Sélectionner une métrique).
5. Choisissez EC2 Spot, Fleet Request Metrics, sélectionnez une métrique (par exemple, TargetCapacity), puis sélectionnez Select metric.

La page Specify metric and conditions (Spécifier les métriques et les conditions) apparaît, présentant un graphique et d'autres informations sur la métrique sélectionnée.

6. Sous Période, choisissez la période d'évaluation de l'alarme, par exemple, 1 minute. Lors de l'évaluation de l'alarme, chaque période est regroupée en un point de données.

Note

Une période plus courte crée une alarme plus sensible.

7. Sous Conditions, définissez l'alarme en définissant la condition de seuil. Par exemple, vous pouvez définir un seuil pour déclencher l'alarme lorsque la valeur de la métrique est supérieure ou égale à 80 %.
8. Sous Additional configuration (Configuration supplémentaire), pour Datapoints to alarm (Points de données pour l'alarme), spécifiez le nombre de points de données (périodes d'évaluation) qui doivent être dans l'état ALARME pour déclencher l'alarme, par exemple, 1 sur 2. Cela

créée une alarme qui passe à l'état ALARME si le seuil est dépassé par ce nombre de périodes consécutives. Pour plus d'informations, consultez la section [Évaluation d'une alarme](#) dans le guide de CloudWatch l'utilisateur Amazon.

9. Pour Missing data treatment (Traitement des données manquantes), choisissez l'une des options (ou conservez la valeur par défaut Treat missing data as missing (Traiter les données manquantes comme manquantes)). Pour plus d'informations, consultez la [section Configuration de la façon dont les CloudWatch alarmes traitent les données manquantes](#) dans le guide de CloudWatch l'utilisateur Amazon.
10. Choisissez Suivant.
11. (Facultatif) Pour recevoir une notification d'un événement de mise à l'échelle, pour Notification, vous pouvez sélectionner ou créer la rubrique Amazon SNS que vous voulez utiliser pour recevoir des notifications. Sinon, vous pouvez supprimer la notification maintenant et en ajouter une plus tard si nécessaire.
12. Choisissez Suivant.
13. Sous Add a description (Ajouter une description), entrez un nom et une description pour l'alarme et choisissez Suivant.
14. Sélectionnez Créer une alarme.

Pour configurer une politique de mise à l'échelle d'étapes pour votre parc d'instances Spot (console)

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot et choisissez Auto Scaling.
4. Si la mise à l'échelle automatique n'est pas configurée, sélectionnez Configurer.
5. Utilisez le champ Scale capacity between (Mettre à l'échelle la capacité entre) pour définir les capacités minimale et maximale de votre parc. Avec les politiques de mise à l'échelle, votre flotte n'aura jamais une capacité inférieure ou supérieure aux limites fixées.
6. Pour Politiques de mise à l'échelle, Type de politique, choisissez Politique de mise à échelles à étapes.
7. À l'origine, la section Politiques de mise à l'échelle contient des politiques de mise à l'échelle nommées ScaleUp et ScaleDown. Vous pouvez compléter ces stratégies ou cliquer sur Remove policy (Supprimer la stratégie) pour les supprimer. Vous pouvez également choisir Add policy (Ajouter une stratégie).

8. Pour définir une politique, procédez comme suit :
 - a. Pour Policy name (Nom de la stratégie), attribuez un nom à cette stratégie.
 - b. Pour Policy Trigger, sélectionnez une alarme existante ou choisissez Create alarm pour ouvrir la CloudWatch console Amazon et créer une alarme.
 - c. Pour Modifier la capacité, définissez le nombre par lequel mettre à l'échelle ainsi que les limites inférieure et supérieure de l'ajustement par étapes. Vous pouvez ajouter ou supprimer un nombre spécifique d'instances ou un pourcentage de la taille de flotte existante, ou définir la flotte sur une taille exacte.

Par exemple, pour créer une politique de mise à l'échelle qui augmente la capacité de la flotte de 30 %, sélectionnez Add, tapez 30 dans le champ suivant, puis cliquez sur percent. Par défaut, la limite inférieure pour l'ajout d'une politique est le seuil de l'alarme et la limite supérieure est l'infini positif (+). Par défaut, la limite supérieure pour la suppression d'une politique est le seuil de l'alarme et la limite inférieure est l'infini négatif (-).

- d. (Facultatif) Pour ajouter une autre étape, cliquez sur Ajouter une étape.
 - e. Pour le Temps de stabilisation, spécifiez une nouvelle valeur (en secondes) ou conservez la valeur par défaut.
9. Choisissez Enregistrer.

Pour configurer des politiques de dimensionnement par étapes pour votre parc de spots à l'aide du AWS CLI

1. Enregistrez la demande de parc d'instances Spot en tant que cible évolutive à l'aide de la commande [register-scalable-target](#).
2. Créez une stratégie de mise à l'échelle à l'aide de la commande [put-scaling-policy](#).
3. Créez une alarme qui déclenche la stratégie de mise à l'échelle à l'aide de la commande [put-metric-alarm](#).

Mise à l'échelle du parc d'instances Spot en utilisant la mise à l'échelle planifiée

La mise à l'échelle en fonction d'une planification vous permet de mettre à l'échelle l'application en réponse aux changements de demande. Pour utiliser la mise à l'échelle planifiée, vous créez des actions planifiées, qui indiquent au parc d'instances Spot d'effectuer des activités de mise à l'échelle à des heures spécifiques. Lorsque vous créez une action planifiée, vous spécifiez le parc d'instances Spot existant, quand l'activité de mise à l'échelle doit avoir lieu, la capacité minimale et la capacité

maximale. Vous pouvez créer des actions planifiées pour une mise à l'échelle unique ou selon une planification récurrente.

Vous ne pouvez créer qu'une action planifiée pour des Parcs d'instances Spot qui existent déjà. Vous ne pouvez pas créer une action planifiée en même temps que vous créez un parc d'instances Spot .

Limitation

La demande de parc d'instances Spot doit être de type `maintain`. La mise à l'échelle automatique n'est pas pris en charge pour les demandes de type `request` et les blocs d'instances Spot.

Pour créer une action planifiée unique

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot, puis choisissez l'onglet Mise à l'échelle planifiée en bas de l'écran.
4. Choisissez Create Scheduled Action (Créer une action planifiée).
5. Pour Nom, spécifiez un nouveau nom pour l'action planifiée.
6. Saisissez une valeur pour Minimum capacity (Capacité minimum), Maximum capacity (Capacité maximum), ou les deux.
7. Pour Recurrence (Récurrence), choisissez Once (Une fois).
8. (Facultatif) Choisissez la date et l'heure pour Heure de début, Heure de fin, ou les deux.
9. Choisissez Submit.

Pour mettre à l'échelle selon un calendrier récurrent

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot, puis choisissez l'onglet Mise à l'échelle planifiée en bas de l'écran.
4. Pour Recurrence (Récurrence), choisissez un des calendriers prédéfinis (par exemple, Every day (Chaque jour)), ou choisissez Custom (Personnalisé) et saisissez une expression CRON. Pour plus d'informations sur les expressions cron prises en charge par le dimensionnement planifié, consultez la section [Expressions cron](#) du guide de l'utilisateur Amazon CloudWatch Events.
5. (Facultatif) Choisissez la date et l'heure pour Heure de début, Heure de fin, ou les deux.

6. Choisissez Submit.

Pour modifier une action planifiée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot, puis choisissez l'onglet Mise à l'échelle planifiée en bas de l'écran.
4. Sélectionnez l'action planifiée et choisissez Actions, Modifier.
5. Apportez les modifications nécessaires et choisissez Soumettre.

Pour supprimer une action planifiée

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Demandes Spot.
3. Sélectionnez votre demande de parc d'instances Spot, puis choisissez l'onglet Mise à l'échelle planifiée en bas de l'écran.
4. Sélectionnez l'action planifiée et choisissez Actions, Supprimer.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour gérer le dimensionnement planifié à l'aide du AWS CLI

Utilisez les commandes suivantes :

- [put-scheduled-action](#)
- [describe-scheduled-actions](#)
- [delete-scheduled-action](#)

Surveillez les événements de votre flotte à l'aide d'Amazon EventBridge

Lorsque l'état d'une flotte EC2 ou Spot change, la flotte émet une notification. La notification est mise à disposition sous la forme d'un événement envoyé à Amazon EventBridge (anciennement Amazon CloudWatch Events). Les événements sont générés dans la mesure du possible.

Avec Amazon EventBridge, vous pouvez créer des règles qui déclenchent des actions programmables en réponse à un événement. Par exemple, vous pouvez créer deux EventBridge règles, l'une qui est déclenchée lorsqu'un état de flotte change, et l'autre qui est déclenchée lorsqu'une instance du parc est résiliée. Vous pouvez configurer la première règle de sorte que, si l'état de la flotte change, la première règle appelle une rubrique SNS pour vous envoyer une notification par e-mail. Vous pouvez configurer la deuxième règle de sorte que, si une instance est résiliée, la règle appelle une fonction Lambda pour lancer une nouvelle instance.

Rubriques

- [Types d'événements de flotte EC2](#)
- [Types d'événements de parc d'instances Spot](#)
- [Créez des EventBridge règles Amazon](#)

Types d'événements de flotte EC2

Note

Seuls les parcs de type `maintain` et `request` émettent des événements. Les parcs de type `instant` n'émettent pas d'événements car elles envoient des demandes uniques synchrones et l'état du parc est connu immédiatement dans la réponse.

Il existe cinq types d'événements de flotte EC2. Pour chaque type d'événement, il existe plusieurs sous-types.

Les événements sont envoyés EventBridge au format JSON. Les champs suivants de l'événement forment le modèle d'événement défini dans la règle et qui déclenchent une action :

```
"source": "aws.ec2fleet"
```

Identifie que l'événement provient de flotte EC2.

```
"detail-type": "EC2 Fleet State Change"
```

Identifie le type d'événement.

```
"detail": { "sub-type": "submitted" }
```

Identifie le sous-type d'événement.

Types d'événements

- [Modification de l'état du flotte EC2](#)
- [Modification de la demande d'instance Spot de flotte EC2](#)
- [Modification de l'instance de flotte EC2](#)
- [Informations sur la flotte EC2](#)
- [Erreur de flotte EC2](#)

Modification de l'état du flotte EC2

EC2 Fleet envoie un `EC2 Fleet State Change` événement à Amazon EventBridge lorsqu'un parc EC2 change d'état.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
  "detail-type": "EC2 Fleet State Change",
  "source": "aws.ec2fleet",
  "account": "123456789012",
  "time": "2020-11-09T09:00:20Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-be4d-6b0809bffff0a"
  ],
  "detail": {
    "sub-type": "active"
  }
}
```

Les valeurs possibles pour `sub-type` sont :

`active`

La demande de flotte EC2 a été validée et Amazon EC2 tente de conserver le nombre cible d'instances en cours d'exécution.

deleted

La demande de flotte EC2 est supprimée et n'a aucune instance en cours d'exécution. La flotte EC2 est supprimée deux jours après la résiliation de ses instances.

deleted_running

La demande de flotte EC2 est supprimée et ne lance pas d'instances supplémentaires. Ses instances existantes continuent de s'exécuter jusqu'à ce qu'elles soient interrompues ou mises hors service. La demande conserve cet état jusqu'à ce que toutes les instances soient interrompues ou mises hors service.

deleted_terminating

La demande de flotte EC2 est supprimée et ses instances sont résiliées. La demande conserve cet état jusqu'à ce que toutes les instances soient mises hors service.

expired

La demande de flotte EC2 a expiré. Si la demande a été créée avec un ensemble `TerminateInstancesWithExpiration`, un événement `terminated` ultérieur indique que les instances sont résiliées.

modify_in_progress

La demande de flotte EC2 est en cours de modification. La demande conserve cet état jusqu'à ce que la modification soit totalement traitée.

modify_succeeded

La demande de flotte EC2 a été modifiée.

submitted

La demande de flotte EC2 est en cours d'évaluation et Amazon EC2 se prépare à lancer le nombre cible d'instances.

progress

La demande de flotte EC2 est en cours d'exécution.

Modification de la demande d'instance Spot de flotte EC2

EC2 Fleet envoie un `EC2 Fleet Spot Instance Request Change` événement à Amazon EventBridge lorsqu'une demande d'instance Spot change d'état dans le parc.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
  "detail-type": "EC2 Fleet Spot Instance Request Change",
  "source": "aws.ec2fleet",
  "account": "123456789012",
  "time": "2020-11-09T09:00:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
  ],
  "detail": {
    "spot-instance-request-id": "sir-rmqske6h",
    "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
cancelled_running",
    "sub-type": "cancelled"
  }
}
```

Les valeurs possibles pour sub-type sont :

active

La demande d'instance Spot a été exécutée et est associée à une instance Spot.

cancelled

Vous avez annulé la demande d'instance Spot ou la demande d'instance Spot a expiré.

disabled

Vous avez arrêté l'instance Spot.

submitted

La demande d'Instance Spot est soumise.

Modification de l'instance de flotte EC2

EC2 Fleet envoie un EC2 Fleet Instance Change événement à Amazon EventBridge lorsqu'une instance de la flotte change d'état.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
  "detail-type": "EC2 Fleet Instance Change",
  "source": "aws.ec2fleet",
  "account": "123456789012",
  "time": "2020-11-09T09:00:23Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bffff0a"
  ],
  "detail": {
    "instance-id": "i-0c594155dd5ff1829",
    "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
    "sub-type": "launched"
  }
}
```

Les valeurs possibles pour sub-type sont :

launched

Une nouvelle instance a été lancée.

terminated

L'instance a été résiliée.

termination_notified

Une notification de résiliation d'instance a été envoyée lorsqu'une instance Spot a été résiliée par Amazon EC2 pendant la réduction d'échelle, lorsque la capacité cible de la flotte a été modifiée à la baisse, par exemple, d'une capacité cible de 4 à une capacité cible de 3.

Informations sur la flotte EC2

EC2 Fleet envoie un EC2 Fleet Information événement à Amazon EventBridge en cas d'erreur lors de l'expédition. L'événement d'information n'empêche pas la flotte de tenter d'atteindre sa capacité cible.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
  "detail-type": "EC2 Fleet Information",
  "source": "aws.ec2fleet",
  "account": "123456789012",
  "time": "2020-11-09T08:17:07Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
  ],
  "detail": {
    "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
    "sub-type": "launchSpecUnusable"
  }
}
```

Les valeurs possibles pour sub-type sont :

`fleetProgressHalted`

Le prix dans chaque spécification de lancement n'est pas valide car il est inférieur au prix Spot (toutes les spécifications de lancement ont produit des événements `launchSpecUnusable`). Une spécification de lancement peut devenir valide si le prix Spot change.

`launchSpecTemporarilyBlacklisted`

La configuration n'est pas valide et plusieurs tentatives de lancement d'instances ont échoué. Pour en savoir plus, consultez la description de l'événement.

`launchSpecUnusable`

Le prix d'une spécification de lancement n'est pas valide car il est inférieur au prix Spot.

`registerWithLoadBalancersFailed`

Une tentative d'enregistrement des instances avec des équilibreurs de charge a échoué. Pour en savoir plus, consultez la description de l'événement.

Erreur de flotte EC2

EC2 Fleet envoie un `EC2 Fleet Error` événement à Amazon EventBridge en cas d'erreur lors de l'expédition. L'événement d'erreur empêche la flotte de tenter d'atteindre sa capacité cible.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
  "detail-type": "EC2 Fleet Error",
  "source": "aws.ec2fleet",
  "account": "123456789012",
  "time": "2020-10-07T01:44:24Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-d33e68eafa08"
  ],
  "detail": {
    "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not supported for the instance type 'm3.large'. ",
    "sub-type": "spotFleetRequestConfigurationInvalid"
  }
}
```

Les valeurs possibles pour `sub-type` sont :

`iamFleetRoleInvalid`

La flotte EC2 ne dispose pas des autorisations requises pour lancer ou résilier une instance.

`allLaunchSpecsTemporarilyBlacklisted`

Aucune des configurations n'est valide et plusieurs tentatives de lancement d'instances ont échoué. Pour en savoir plus, consultez la description de l'événement.

`spotInstanceCountLimitExceeded`

Vous avez atteint la limite du nombre d'instances Spot que vous pouvez lancer.

`spotFleetRequestConfigurationInvalid`

La configuration n'est pas valide. Pour en savoir plus, consultez la description de l'événement.

Types d'événements de parc d'instances Spot

Il existe cinq types d'événements de parc d'instances Spot . Pour chaque type d'événement, il existe plusieurs sous-types.

Les événements sont envoyés EventBridge au format JSON. Les champs suivants de l'événement forment le modèle d'événement défini dans la règle et qui déclenchent une action :

```
"source": "aws.ec2spotfleet"
```

Identifie que l'événement provient d'un parc d'instances Spot.

```
"detail-type": "EC2 Spot Fleet State Change"
```

Identifie le type d'événement.

```
"detail": { "sub-type": "submitted" }
```

Identifie le sous-type d'événement.

Types d'événements

- [Changement d'état du parc d'instances Spot EC2](#)
- [Modification de la demande d'instance Spot de flotte EC2](#)
- [Modification de l'instance de parc d'instances Spot EC2](#)
- [Informations sur le parc d'instances Spot EC2](#)
- [Erreur de parc d'instances Spot EC2](#)

Changement d'état du parc d'instances Spot EC2

Spot Fleet envoie un EC2 Spot Fleet State Change événement à Amazon EventBridge lorsqu'un Spot Fleet change d'état.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
  "detail-type": "EC2 Spot Fleet State Change",
  "source": "aws.ec2spotfleet",
  "account": "123456789012",
```

```
"time": "2020-11-09T08:57:06Z",
"region": "us-east-1",
"resources": [
  "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
],
"detail": {
  "sub-type": "submitted"
}
}
```

Les valeurs possibles pour sub-type sont :

active

La demande de parc d'instances Spot a été validée et Amazon EC2 tente de conserver le nombre cible d'instances en cours d'exécution.

cancelled

La demande de parc d'instances Spot est annulée et n'a aucune instance en cours d'exécution. Le parc d'instances sera supprimé deux jours après la résiliation de ses instances.

cancelled_running

La demande de parc d'instances Spot est annulée et ne lance pas d'instances supplémentaires. Ses instances existantes continuent de s'exécuter jusqu'à ce qu'elles soient interrompues ou mises hors service. La demande conserve cet état jusqu'à ce que toutes les instances soient interrompues ou mises hors service.

cancelled_terminating

La demande de parc d'instances Spot est annulée et ses instances sont résiliées. La demande conserve cet état jusqu'à ce que toutes les instances soient mises hors service.

expired

La demande de parc d'instances Spot a expiré. Si la demande a été créée avec un ensemble `TerminateInstancesWithExpiration`, un événement `terminated` ultérieur indique que les instances sont résiliées.

modify_in_progress

La demande de parc d'instances Spot est en cours de modification. La demande conserve cet état jusqu'à ce que la modification soit totalement traitée.

modify_succeeded

La demande de parc d'instances Spot a été modifiée.

submitted

La demande de parc d'instances Spot est en cours d'évaluation et Amazon EC2 se prépare à lancer le nombre cible d'instances.

progress

La demande de parc d'instances Spot est en cours d'exécution.

Modification de la demande d'instance Spot de flotte EC2

Spot Fleet envoie un EC2 Spot Fleet Spot Instance Request Change événement à Amazon EventBridge lorsqu'une demande d'instance Spot change d'état dans le parc.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
  "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
  "source": "aws.ec2spotfleet",
  "account": "123456789012",
  "time": "2020-11-09T08:53:21Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
  ],
  "detail": {
    "spot-instance-request-id": "sir-a2w9gc5h",
    "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
cancelled_running",
    "sub-type": "cancelled"
  }
}
```

Les valeurs possibles pour sub-type sont :

active

La demande d'instance Spot a été exécutée et est associée à une instance Spot.

cancelled

Vous avez annulé la demande d'instance Spot ou la demande d'instance Spot a expiré.

disabled

Vous avez arrêté l'instance Spot.

submitted

La demande d'Instance Spot est soumise.

Modification de l'instance de parc d'instances Spot EC2

Spot Fleet envoie un EC2 Spot Fleet Instance Change événement à Amazon EventBridge lorsqu'une instance du parc change d'état.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
  "detail-type": "EC2 Spot Fleet Instance Change",
  "source": "aws.ec2spotfleet",
  "account": "123456789012",
  "time": "2020-11-09T07:25:02Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-af9c-0095e6e3ba61"
  ],
  "detail": {
    "instance-id": "i-08b90df1e09c30c9b",
    "description": "{\"instanceType\": \"r4.2xlarge\", \"image\": \"ami-032930428bf1abbff\", \"productDescription\": \"Linux/UNIX\", \"availabilityZone\": \"us-east-1a\"}",
    "sub-type": "launched"
  }
}
```

Les valeurs possibles pour sub-type sont :

launched

Une nouvelle instance a été lancée.

terminated

L'instance a été résiliée.

termination_notified

Une notification de résiliation d'instance a été envoyée lorsqu'une instance Spot a été résiliée par Amazon EC2 pendant la réduction d'échelle, lorsque la capacité cible de la flotte a été modifiée à la baisse, par exemple, d'une capacité cible de 4 à une capacité cible de 3.

Informations sur le parc d'instances Spot EC2

Spot Fleet envoie un EC2 Spot Fleet Information événement à Amazon EventBridge en cas d'erreur lors de l'expédition. L'événement d'information n'empêche pas la flotte de tenter d'atteindre sa capacité cible.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
  "detail-type": "EC2 Spot Fleet Information",
  "source": "aws.ec2spotfleet",
  "account": "123456789012",
  "time": "2020-11-08T20:56:12Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-af18-4647-8757-7d69c94971b1"
  ],
  "detail": {
    "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot bid price is less than Spot market price $0.5291",
    "sub-type": "launchSpecUnusable"
  }
}
```

Les valeurs possibles pour sub-type sont :

fleetProgressHalted

Le prix dans chaque spécification de lancement n'est pas valide car il est inférieur au prix Spot (toutes les spécifications de lancement ont produit des événements `launchSpecUnusable`). Une spécification de lancement peut devenir valide si le prix Spot change.

launchSpecTemporarilyBlacklisted

La configuration n'est pas valide et plusieurs tentatives de lancement d'instances ont échoué. Pour en savoir plus, consultez la description de l'événement.

launchSpecUnusable

Le prix d'une spécification de lancement n'est pas valide car il est inférieur au prix Spot.

registerWithLoadBalancersFailed

Une tentative d'enregistrement des instances avec des équilibreurs de charge a échoué. Pour en savoir plus, consultez la description de l'événement.

Erreur de parc d'instances Spot EC2

Spot Fleet envoie un `EC2 Spot Fleet Error` événement à Amazon EventBridge en cas d'erreur lors de l'expédition. L'événement d'erreur empêche la flotte de tenter d'atteindre sa capacité cible.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
  "detail-type": "EC2 Spot Fleet Error",
  "source": "aws.ec2spotfleet",
  "account": "123456789012",
  "time": "2020-11-09T06:56:07Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
  ],
  "detail": {
    "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
associatePublicIPAddress parameter can only be specified for the network interface
with DeviceIndex 0. ",
    "sub-type": "spotFleetRequestConfigurationInvalid"
  }
}
```

```
}  
}
```

Les valeurs possibles pour sub-type sont :

`iamFleetRoleInvalid`

Le parc d'instances Spot ne dispose pas des autorisations requises pour lancer ou résilier une instance.

`allLaunchSpecsTemporarilyBlacklisted`

Aucune des configurations n'est valide et plusieurs tentatives de lancement d'instances ont échoué. Pour en savoir plus, consultez la description de l'événement.

`spotInstanceCountLimitExceeded`

Vous avez atteint la limite du nombre d'instances Spot que vous pouvez lancer.

`spotFleetRequestConfigurationInvalid`

La configuration n'est pas valide. Pour en savoir plus, consultez la description de l'événement.

Créez des EventBridge règles Amazon

Lorsqu'une notification de changement d'état est émise pour une flotte EC2 ou une flotte ponctuelle, l'événement correspondant à la notification est envoyé à Amazon EventBridge. S'il EventBridge détecte un modèle d'événement correspondant à un modèle défini dans une règle, EventBridge invoque une cible (ou des cibles) spécifiée dans la règle.

Vous pouvez écrire une EventBridge règle et automatiser les actions à effectuer lorsque le modèle d'événement correspond à la règle.

Rubriques

- [Créez des EventBridge règles Amazon pour surveiller les événements de la flotte EC2](#)
- [Créez des EventBridge règles Amazon pour surveiller les événements de Spot Fleet](#)

Créez des EventBridge règles Amazon pour surveiller les événements de la flotte EC2

Lorsqu'une notification de changement d'état est émise pour une flotte EC2, l'événement correspondant à la notification est envoyé à Amazon EventBridge sous la forme d'un fichier JSON.

Vous pouvez écrire une EventBridge règle pour automatiser les actions à effectuer lorsqu'un modèle d'événement correspond à la règle. S'il EventBridge détecte un modèle d'événement correspondant à un modèle défini dans une règle, EventBridge invoque la cible (ou les cibles) spécifiée dans la règle.

Les champs suivants forment le modèle d'événement défini dans la règle :

```
"source": "aws.ec2fleet"
```

Identifie que l'événement provient de flotte EC2.

```
"detail-type": "EC2 Fleet State Change"
```

Identifie le type d'événement.

```
"detail": { "sub-type": "submitted" }
```

Identifie le sous-type d'événement.

Pour obtenir la liste des événements de flotte EC2 et des exemples de données d'événement, consultez [the section called “Types d'événements de flotte EC2”](#).

Exemples

- [Création d'une EventBridge règle pour envoyer une notification](#)
- [Création d'une EventBridge règle pour déclencher une fonction Lambda](#)

Création d'une EventBridge règle pour envoyer une notification

L'exemple suivant crée une EventBridge règle pour envoyer un e-mail, un SMS ou une notification push mobile chaque fois qu'Amazon EC2 émet une notification de modification de l'état de la flotte EC2. Le signal de cet exemple est émis en tant qu'événement de EC2 Fleet State Change, ce qui déclenche l'action définie par la règle.

Avant de créer la EventBridge règle, vous devez créer la rubrique Amazon SNS pour l'e-mail, le message texte ou la notification push mobile.

Pour créer une EventBridge règle permettant d'envoyer une notification lorsque l'état d'une flotte EC2 change

1. Ouvrez la EventBridge console Amazon à l'[adresse https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Choisissez Créer une règle.
3. Pour Define rule detail (Définir les détails de la règle), procédez comme suit :

- a. Entrez un nom et éventuellement une description pour la règle.

Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

- b. Pour Event bus (Bus d'événement), choisissez default (défaut). Lorsqu'un service AWS de votre compte génère un événement, il accède toujours au bus d'événement par défaut de votre compte.
 - c. Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
 - d. Choisissez Suivant.
4. Pour Build event pattern (Créer un modèle d'événement), procédez comme suit :
 - a. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.
 - b. Pour le Event pattern (Modèle d'événement), dans cet exemple, vous spécifierez le modèle d'événement suivant pour correspondre à l'événement EC2 Fleet Instance Change.

```
{
  "source": ["aws.ec2fleet"],
  "detail-type": ["EC2 Fleet Instance Change"]
}
```

Pour ajouter le modèle d'événement, vous pouvez utiliser un modèle en choisissant Event pattern form (Formulaire de modèle d'événement), ou spécifiez votre propre modèle en choisissant Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]), comme suit :

- i. Pour utiliser un modèle pour créer le modèle d'événement, procédez comme suit :
 - A. Sélectionnez Event pattern form (Formulaire de modèle d'événement).
 - B. Pour Event source (Origine de l'événement), choisissez AWS services (Services).
 - C. Pour Service AWS, choisissez EC2 Fleet.
 - D. Pour Event type (Type d'événement), choisissez EC2 Fleet Instance Change (Modification de l'instance de flotte EC2).
 - E. Pour personnaliser le modèle, choisissez Edit pattern (Modifier le modèle) et apportez vos modifications pour correspondre à l'exemple de modèle d'événement.

- ii. (Alternative) Pour spécifier un modèle d'événement personnalisé, procédez comme suit :
 - A. Choisissez Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]).
 - B. Dans la boîte de dialogue Event pattern (Modèle d'événement), ajoutez le modèle d'événement pour cet exemple.
- c. Choisissez Next (Suivant).
5. Pour Select target(s) (Sélectionner la ou les cibles), procédez comme suit :
 - a. Pour Types de cibles, choisissez service AWS .
 - b. Pour Select a target (Sélectionner une cible), sélectionnez SNS topic (Rubrique SNS) pour envoyer un e-mail, un SMS ou une notification push mobile lorsque l'événement se produit.
 - c. Pour Topic (Rubrique), sélectionnez une rubrique existante. Vous devez d'abord créer une rubrique Amazon SNS à l'aide de la console Amazon SNS. Pour plus d'informations, consultez la section [Utilisation d'Amazon SNS pour la messagerie application-to-person \(A2P\) dans le manuel](#) du développeur Amazon Simple Notification Service.
 - d. (Facultatif) Sous Additional settings (Paramètres supplémentaires), vous pouvez configurer des paramètres supplémentaires. Pour plus d'informations, consultez la section [Création de EventBridge règles Amazon réagissant aux événements](#) (étape 16) dans le guide de EventBridge l'utilisateur Amazon.
 - e. Choisissez Suivant.
6. (Facultatif) Pour Tags (Identifications), vous pouvez également attribuer une ou plusieurs identifications à votre règle, puis choisir Next (Suivant).
7. Pour Review and create (Vérifier et créer), procédez comme suit :
 - a. Consultez les détails de la règle et modifiez-les si nécessaire.
 - b. Choisissez Créer une règle.

Pour plus d'informations, consultez les [EventBridge règles Amazon et les modèles d' EventBridge événements Amazon](#) dans le guide de EventBridge l'utilisateur Amazon

Création d'une EventBridge règle pour déclencher une fonction Lambda

L'exemple suivant crée une EventBridge règle pour déclencher une fonction Lambda chaque fois qu'Amazon EC2 émet une notification de modification d'instance EC2 Fleet lors du lancement d'une

instance. Le signal de cet exemple est émis en tant qu'événement EC2 Fleet Instance Change, de sous-type `launched`, ce qui déclenche l'action définie par la règle.

Avant de créer la EventBridge règle, vous devez créer la fonction Lambda.

Pour créer la fonction Lambda à utiliser dans la règle EventBridge

1. Ouvrez la AWS Lambda console à l'[adresse https://console.aws.amazon.com/lambda/](https://console.aws.amazon.com/lambda/).
2. Sélectionnez Créer une fonction.
3. Saisissez un nom pour votre fonction, configurez le code, puis sélectionnez Create function (Créer une fonction).

Pour plus d'informations sur l'utilisation de Lambda, consultez [Créer une fonction Lambda avec la console](#) dans le AWS Lambda Guide du développeur.

Pour créer une EventBridge règle permettant de déclencher une fonction Lambda lorsqu'une instance d'un parc EC2 change d'état

1. Ouvrez la EventBridge console Amazon à l'[adresse https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Choisissez Créer une règle.
3. Pour Define rule detail (Définir les détails de la règle), procédez comme suit :
 - a. Entrez un nom et éventuellement une description pour la règle.

Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

- b. Pour Event bus (Bus d'événement), choisissez default (défaut). Lorsqu'un service AWS de votre compte génère un événement, il accède toujours au bus d'événement par défaut de votre compte.
 - c. Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
 - d. Choisissez Suivant.
4. Pour Build event pattern (Créer un modèle d'événement), procédez comme suit :
 - a. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.

- b. Pour Event pattern (Modèle d'événement), pour cet exemple, vous allez spécifier le modèle d'événement suivant pour correspondre à l'événement EC2 Fleet Instance Change et au sous-type launched.

```
{
  "source": ["aws.ec2fleet"],
  "detail-type": ["EC2 Fleet Instance Change"],
  "detail": {
    "sub-type": ["launched"]
  }
}
```

Pour ajouter le modèle d'événement, vous pouvez utiliser un modèle en choisissant Event pattern form (Formulaire de modèle d'événement), ou spécifiez votre propre modèle en choisissant Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]), comme suit :

- i. Pour utiliser un modèle pour créer le modèle d'événement, procédez comme suit :
 - A. Sélectionnez Event pattern form (Formulaire de modèle d'événement).
 - B. Pour Event source (Origine de l'événement), choisissez AWS services (Services).
 - C. Pour Service AWS , choisissez EC2 Fleet.
 - D. Pour Event type (Type d'événement), choisissez EC2 Fleet Instance Change (Modification de l'instance de flotte EC2).
 - E. Choisissez Edit pattern (Modifier le modèle), et ajoutez "detail": {"sub-type": ["launched"]} pour correspondre à l'exemple de modèle d'événement. Pour un format JSON approprié, insérez une virgule (,) après le crochet carré précédent (]).
 - ii. (Alternative) Pour spécifier un modèle d'événement personnalisé, procédez comme suit :
 - A. Choisissez Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]).
 - B. Dans la boîte de dialogue Event pattern (Modèle d'événement), ajoutez le modèle d'événement pour cet exemple.
- c. Choisissez Next (Suivant).
5. Pour Select target(s) (Sélectionner la ou les cibles), procédez comme suit :
 - a. Pour Types de cibles, choisissez service AWS .

- b. Pour Select a target (Sélectionner une cible), sélectionnez SNS topic (Rubrique SNS) pour envoyer un e-mail, un SMS ou une notification push mobile lorsque l'événement se produit.
 - c. Pour Topic (Rubrique), sélectionnez Lambda function (Fonction Lambda) et, pour Function (Fonction), sélectionnez la fonction que vous avez créée pour répondre lorsque l'événement se produit.
 - d. (Facultatif) Sous Additional settings (Paramètres supplémentaires), vous pouvez configurer des paramètres supplémentaires. Pour plus d'informations, consultez la section [Création de EventBridge règles Amazon réagissant aux événements](#) (étape 16) dans le guide de EventBridge l'utilisateur Amazon.
 - e. Choisissez Suivant.
6. (Facultatif) Pour Tags (Identifications), vous pouvez également attribuer une ou plusieurs identifications à votre règle, puis choisir Next (Suivant).
 7. Pour Review and create (Vérifier et créer), procédez comme suit :
 - a. Consultez les détails de la règle et modifiez-les si nécessaire.
 - b. Choisissez Créer une règle.

Pour un didacticiel sur la création d'une fonction Lambda et d'une EventBridge règle qui exécute la fonction Lambda, voir [Tutoriel : enregistrer l'état d'une instance Amazon EC2 à l'aide du manuel du développeur](#). EventBridge AWS Lambda

Créez des EventBridge règles Amazon pour surveiller les événements de Spot Fleet

Lorsqu'une notification de changement d'état est émise pour un parc de spots, l'événement correspondant à la notification est envoyé à Amazon EventBridge sous la forme d'un fichier JSON. Vous pouvez écrire une EventBridge règle pour automatiser les actions à effectuer lorsqu'un modèle d'événement correspond à la règle. S'il EventBridge détecte un modèle d'événement correspondant à un modèle défini dans une règle, EventBridge invoque la cible (ou les cibles) spécifiée dans la règle.

Les champs suivants forment le modèle d'événement défini dans la règle :

```
"source": "aws.ec2spotfleet"
```

Identifie que l'événement provient d'un parc d'instances Spot.

```
"detail-type": "EC2 Spot Fleet State Change"
```

Identifie le type d'événement.

```
"detail": { "sub-type": "submitted" }
```

Identifie le sous-type d'événement.

Pour obtenir la liste des événements de parc d'instances Spot et des exemples de données d'événement, consultez [the section called "Types d'événements de parc d'instances Spot"](#).

Exemples

- [Création d'une EventBridge règle pour envoyer une notification](#)
- [Création d'une EventBridge règle pour déclencher une fonction Lambda](#)

Création d'une EventBridge règle pour envoyer une notification

L'exemple suivant crée une EventBridge règle pour envoyer un e-mail, un SMS ou une notification push mobile chaque fois qu'Amazon EC2 émet une notification de changement d'état de Spot Fleet. Le signal de cet exemple est émis en tant qu'événement de EC2 Spot Fleet State Change, ce qui déclenche l'action définie par la règle. Avant de créer la EventBridge règle, vous devez créer la rubrique Amazon SNS pour l'e-mail, le message texte ou la notification push mobile.

Pour créer une EventBridge règle permettant d'envoyer une notification lorsqu'un état de Spot Fleet change

1. Ouvrez la EventBridge console Amazon à l'[adresse https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Choisissez Créer une règle.
3. Pour Define rule detail (Définir les détails de la règle), procédez comme suit :

- a. Entrez un nom et éventuellement une description pour la règle.

Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

- b. Pour Event bus (Bus d'événement), choisissez default (défaut). Lorsqu'un service AWS de votre compte génère un événement, il accède toujours au bus d'événement par défaut de votre compte.
 - c. Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
 - d. Choisissez Suivant.
4. Pour Build event pattern (Créer un modèle d'événement), procédez comme suit :

- a. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.
- b. Pour le Event pattern (Modèle d'événement), dans cet exemple, vous spécifierez le modèle d'événement suivant pour correspondre à l'événement EC2 Spot Fleet Instance Change.

```
{  
  "source": ["aws.ec2spotfleet"],  
  "detail-type": ["EC2 Spot Fleet Instance Change"]  
}
```

Pour ajouter le modèle d'événement, vous pouvez utiliser un modèle en choisissant Event pattern form (Formulaire de modèle d'événement), ou spécifiez votre propre modèle en choisissant Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]), comme suit :

- i. Pour utiliser un modèle pour créer le modèle d'événement, procédez comme suit :
 - A. Sélectionnez Event pattern form (Formulaire de modèle d'événement).
 - B. Pour Event source (Origine de l'événement), choisissez AWS services (Services).
 - C. Pour Service AWS , choisissez Parc d'instances Spot EC2.
 - D. Pour Event type (Type d'événement), choisissez EC2 Spot Fleet Instance Change (Modification du parc d'instances Spot EC2).
 - E. Pour personnaliser le modèle, choisissez Edit pattern (Modifier le modèle) et apportez vos modifications pour correspondre à l'exemple de modèle d'événement.
 - ii. (Alternative) Pour spécifier un modèle d'événement personnalisé, procédez comme suit :
 - A. Choisissez Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]).
 - B. Dans la boîte de dialogue Event pattern (Modèle d'événement), ajoutez le modèle d'événement pour cet exemple.
- c. Choisissez Next (Suivant).
5. Pour Select target(s) (Sélectionner la ou les cibles), procédez comme suit :
 - a. Pour Types de cibles, choisissez service AWS .

- b. Pour Select a target (Sélectionner une cible), sélectionnez SNS topic (Rubrique SNS) pour envoyer un e-mail, un SMS ou une notification push mobile lorsque l'événement se produit.
 - c. Pour Topic (Rubrique), sélectionnez une rubrique existante. Vous devez d'abord créer une rubrique Amazon SNS à l'aide de la console Amazon SNS. Pour plus d'informations, consultez la section [Utilisation d'Amazon SNS pour la messagerie application-to-person \(A2P\) dans le manuel](#) du développeur Amazon Simple Notification Service.
 - d. (Facultatif) Sous Additional settings (Paramètres supplémentaires), vous pouvez configurer des paramètres supplémentaires. Pour plus d'informations, consultez la section [Création de EventBridge règles Amazon réagissant aux événements](#) (étape 16) dans le guide de EventBridge l'utilisateur Amazon.
 - e. Choisissez Suivant.
6. (Facultatif) Pour Tags (Identifications), vous pouvez également attribuer une ou plusieurs identifications à votre règle, puis choisir Next (Suivant).
 7. Pour Review and create (Vérifier et créer), procédez comme suit :
 - a. Consultez les détails de la règle et modifiez-les si nécessaire.
 - b. Choisissez Créer une règle.

Pour plus d'informations, consultez les [EventBridge règles Amazon et les modèles d' EventBridge événements Amazon](#) dans le guide de EventBridge l'utilisateur Amazon

Création d'une EventBridge règle pour déclencher une fonction Lambda

L'exemple suivant crée une EventBridge règle pour déclencher une fonction Lambda chaque fois qu'Amazon EC2 émet une notification de modification d'instance Spot Fleet lors du lancement d'une instance. Le signal de cet exemple est émis en tant qu'événement EC2 Spot Fleet Instance Change, de sous-type Launched, ce qui déclenche l'action définie par la règle.

Avant de créer la EventBridge règle, vous devez créer la fonction Lambda.

Pour créer la fonction Lambda à utiliser dans la règle EventBridge

1. Ouvrez la AWS Lambda console à l'[adresse https://console.aws.amazon.com/lambda/](https://console.aws.amazon.com/lambda/).
2. Sélectionnez Créer une fonction.
3. Saisissez un nom pour votre fonction, configurez le code, puis sélectionnez Create function (Créer une fonction).

Pour plus d'informations sur l'utilisation de Lambda, consultez [Créer une fonction Lambda avec la console](#) dans le AWS Lambda Guide du développeur.

Pour créer une EventBridge règle afin de déclencher une fonction Lambda lorsqu'une instance d'un parc Spot change d'état

1. Ouvrez la EventBridge console Amazon à l'[adresse https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Choisissez Créer une règle.
3. Pour Define rule detail (Définir les détails de la règle), procédez comme suit :

- a. Entrez un nom et éventuellement une description pour la règle.

Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

- b. Pour Event bus (Bus d'événement), choisissez default (défaut). Lorsqu'un service AWS de votre compte génère un événement, il accède toujours au bus d'événement par défaut de votre compte.
 - c. Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
 - d. Choisissez Suivant.
4. Pour Build event pattern (Créer un modèle d'événement), procédez comme suit :

- a. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.
- b. Pour Event pattern (Modèle d'événement), pour cet exemple, vous allez spécifier le modèle d'événement suivant pour correspondre à l'événement EC2 Spot Fleet Instance Change et au sous-type launched.

```
{
  "source": ["aws.ec2spotfleet"],
  "detail-type": ["EC2 Spot Fleet Instance Change"],
  "detail": {
    "sub-type": ["launched"]
  }
}
```

Pour ajouter le modèle d'événement, vous pouvez utiliser un modèle en choisissant Event pattern form (Formulaire de modèle d'événement), ou spécifiez votre propre modèle en choisissant Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]), comme suit :

- i. Pour utiliser un modèle pour créer le modèle d'événement, procédez comme suit :
 - A. Sélectionnez Event pattern form (Formulaire de modèle d'événement).
 - B. Pour Event source (Origine de l'événement), choisissez AWS services (Services).
 - C. Pour Service AWS, choisissez Parc d'instances Spot EC2.
 - D. Pour Event type (Type d'événement), choisissez EC2 Spot Fleet Instance Change (Modification du parc d'instances Spot EC2).
 - E. Choisissez Edit pattern (Modifier le modèle), et ajoutez "detail": {"sub-type": ["launched"]} pour correspondre à l'exemple de modèle d'événement. Pour un format JSON approprié, insérez une virgule (,) après le crochet carré précédent (]).
 - ii. (Alternative) Pour spécifier un modèle d'événement personnalisé, procédez comme suit :
 - A. Choisissez Custom pattern (JSON editor) (Modèle personnalisé [éditeur JSON]).
 - B. Dans la boîte de dialogue Event pattern (Modèle d'événement), ajoutez le modèle d'événement pour cet exemple.
 - c. Choisissez Next (Suivant).
5. Pour Select target(s) (Sélectionner la ou les cibles), procédez comme suit :
- a. Pour Types de cibles, choisissez service AWS.
 - b. Pour Select a target (Sélectionner une cible), sélectionnez SNS topic (Rubrique SNS) pour envoyer un e-mail, un SMS ou une notification push mobile lorsque l'événement se produit.
 - c. Pour Topic (Rubrique), sélectionnez Lambda function (Fonction Lambda) et, pour Fonction (Fonction), sélectionnez la fonction que vous avez créée pour répondre lorsque l'événement se produit.
 - d. (Facultatif) Sous Additional settings (Paramètres supplémentaires), vous pouvez configurer des paramètres supplémentaires. Pour plus d'informations, consultez la section [Création de EventBridge règles Amazon réagissant aux événements](#) (étape 16) dans le guide de EventBridge l'utilisateur Amazon.

- e. Choisissez Suivant.
6. (Facultatif) Pour Tags (Identifications), vous pouvez également attribuer une ou plusieurs identifications à votre règle, puis choisir Next (Suivant).
7. Pour Review and create (Vérifier et créer), procédez comme suit :
 - a. Consultez les détails de la règle et modifiez-les si nécessaire.
 - b. Choisissez Créer une règle.

Pour un didacticiel sur la création d'une fonction Lambda et d'une EventBridge règle qui exécute la fonction Lambda, voir [Tutoriel : enregistrer l'état d'une instance Amazon EC2 à l'aide du manuel du développeur](#). EventBridge AWS Lambda

Tutoriels pour les flottes d'instances EC2 et Spot

Les didacticiels suivants vous expliquent les processus courants de création de flottes d'instances EC2 et Spot.

Didacticiels

- [Didacticiel : Utiliser une flotte EC2 avec pondération des instances](#)
- [Didacticiel : Utiliser une flotte EC2 avec la capacité à la demande comme capacité principale](#)
- [Didacticiel : Lancer des instances à la demande en utilisant les réservations de capacité ciblées](#)
- [Tutoriel : Lancer des instances dans des blocs de capacité](#)
- [Didacticiel : utiliser un flotte d'instances EC2 avec pondération des instances](#)

Didacticiel : Utiliser une flotte EC2 avec pondération des instances

Cette procédure utilise une société fictive nommée Example Corp pour illustrer le processus de demande d'une flotte EC2 utilisant la pondération des instances.

Objectif

Example Corp est une entreprise pharmaceutique qui souhaite utiliser la puissance de calcul d'Amazon EC2 pour analyser les composants chimiques susceptibles d'être utilisés dans la lutte contre le cancer.

Planification

Exemple Corp commence par examiner les [bonnes pratiques en matière d'instances Spot](#). Ensuite, Exemple Corp détermine les exigences suivantes pour son flotte EC2.

Types d'instance

Exemple Corp a une application qui exige beaucoup de calculs et de mémoire. Pour un fonctionnement optimal, cette application a besoin d'au moins 60 Go de mémoire et de huit UC virtuelles (vCPU). L'entreprise souhaite optimiser ces ressources pour l'application au prix le plus bas possible. Exemple Corp décide que l'un des types d'instance EC2 suivants est capable de répondre à ses besoins :

Type d'instance	Mémoire (Go)	vCPU
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacité cible en unités

Avec la pondération des instances, la capacité cible peut être égale à un certain nombre d'instances (valeur par défaut) ou à une combinaison de facteurs tels que les cœurs (vCPU), la mémoire GiBs () et le stockage (Go). En considérant que la base de son application (60 Go de RAM et huit vCPU) compte pour une unité, Exemple Corp décide que 20 fois cette quantité suffirait pour répondre à ses besoins. L'entreprise définit donc la capacité cible de sa demande de flotte EC2 sur 20.

Pondérations d'instance

Après avoir déterminé sa capacité cible, Exemple Corp calcule ses pondérations d'instance. Pour calculer la pondération de chaque type d'instance, l'entreprise détermine les unités de chaque type d'instance nécessaires pour atteindre la capacité cible de la façon suivante :

- r3.2xlarge (61,0 Go, 8 vCPU) = 1 unité de 20
- r3.4xlarge (122,0 Go, 16 vCPU) = 2 unités de 20

- r3.8xlarge (244 Go, 32 vCPU) = 4 unités de 20

Par conséquent, Example Corp assigne des pondérations d'instance de 1, 2 et 4 aux configurations de lancement respectives dans sa demande de flotte EC2.

Prix par heure d'unité

Example Corp utilise le [prix à la Demande](#) par heure d'instance comme point de départ de son prix. Elle peut également utiliser les prix Spot récents ou une combinaison des deux. Pour calculer le prix par heure d'unité, elle divise le prix de départ basé sur l'heure d'instance par la pondération.

Exemples :

Type d'instance	Prix à la Demande	Pondération de l'instance	Prix par heure d'unité
r3.2xLarge	0,7 USD	1	0,7 USD
r3.4xLarge	1,4 USD	2	0,7 USD
r3.8xLarge	2.8 USD	4	0,7 USD

Example Corp peut utiliser un prix global par heure d'unité s'élevant à 0,7 USD et rester concurrentielle pour les trois types d'instance. Elle peut également utiliser un prix global par heure d'unité s'élevant à 0,7 USD et un prix spécifique par heure d'unité de 0,9 USD dans la spécification de lancement du type d'instance r3.8xlarge.

Vérifier les autorisations

Avant de créer une flotte EC2, la société Example Corp vérifie qu'elle dispose d'un rôle IAM avec les autorisations requises. Pour plus d'informations, consultez [Conditions préalables requises flotte EC2](#).

Créer un modèle de lancement

Ensuite, Example Corp crée un modèle de lancement. L'ID de modèle de lancement est utilisé à l'étape suivante. Pour plus d'informations, consultez [Création d'un modèle de lancement](#).

Créer la flotte EC2

Exemple Corp crée un fichier, `config.json`, avec la configuration suivante pour son Flotte EC2. Dans l'exemple suivant, remplacez les identificateurs de ressources par vos propres identificateurs de ressources.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-07b3bc7625cdab851",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-482e4972",
          "WeightedCapacity": 1
        },
        {
          "InstanceType": "r3.4xlarge",
          "SubnetId": "subnet-482e4972",
          "WeightedCapacity": 2
        },
        {
          "InstanceType": "r3.8xlarge",
          "MaxPrice": "0.90",
          "SubnetId": "subnet-482e4972",
          "WeightedCapacity": 4
        }
      ]
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
  }
}
```

Exemple Corp crée le Flotte EC2 à l'aide de la commande [create-fleet](#) suivante.

```
aws ec2 create-fleet \
```

```
--cli-input-json file://config.json
```

Pour plus d'informations, consultez [Créer une flotte EC2](#).

Exécution

La stratégie d'allocation détermine de quels groupes de capacités Spot sont issues vos instances Spot.

Avec la stratégie `lowest-price` (qui est la stratégie par défaut), les Instances Spot sont issues du groupe ayant le prix par unité le plus bas au moment de l'exécution. Pour fournir 20 unités de capacité, le Flotte EC2 lance 20 instances `r3.2xlarge` (20 divisé par 1), 10 instances `r3.4xlarge` (20 divisé par 2) ou 5 instances `r3.8xlarge` (20 divisé par 4).

Si Example Corp avait utilisé la stratégie `diversified`, les Instances Spot auraient été issues des trois groupes. Le Flotte EC2 aurait lancé 6 instances `r3.2xlarge` (soit 6 unités), 3 instances `r3.4xlarge` (soit 6 unités) et 2 instances `r3.8xlarge` (soit 8 unités), pour un total de 20 unités.

Didacticiel : Utiliser une flotte EC2 avec la capacité à la demande comme capacité principale

Ce didacticiel utilise une société fictive nommée ABC Online pour illustrer le processus de demande d'une flotte EC2 avec la capacité à la demande comme capacité principale, et la capacité des instances spot si elle est disponible.

Objectif

ABC Online est une compagnie de livraison de restaurants qui veut être capable d'allouer une capacité d'Amazon EC2 entre les types d'instance EC2 et les options d'achat pour atteindre l'échelle, la performance et le coût qu'elle s'est fixés.

Plan

ABC Online nécessite une capacité fixe pour faire face aux périodes de pic, mais souhaiterait bénéficier d'une capacité augmentée pour un prix inférieur. ABC Online détermine les exigences suivantes pour son flotte EC2 :

- Capacité d'instance à la demande : ABC Online nécessite 15 instances à la demande pour s'assurer de pouvoir prendre en charge le trafic dans les périodes de pic.

- Capacité d'instance Spot : ABC Online souhaite améliorer la performance, mais pour un prix inférieur, en mettant en service 5 instances Spot.

Vérifier les autorisations

Avant de créer une flotte EC2, la société ABC Online vérifie qu'elle dispose d'un rôle IAM avec les autorisations requises. Pour plus d'informations, consultez [Conditions préalables requises flotte EC2](#).

Créer un modèle de lancement

Ensuite, ABC Online crée un modèle de lancement. L'ID de modèle de lancement est utilisé à l'étape suivante. Pour plus d'informations, consultez [Création d'un modèle de lancement](#).

Créer la flotte EC2

ABC Online crée un fichier, `config.json`, avec la configuration suivante pour son Flotte EC2. Dans l'exemple suivant, remplacez les identificateurs de ressources par vos propres identificateurs de ressources.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-07b3bc7625cdab851",
        "Version": "2"
      }
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "OnDemandTargetCapacity": 15,
    "DefaultTargetCapacityType": "spot"
  }
}
```

ABC Online crée la Flotte EC2 à l'aide de la commande [create-fleet](#) suivante.

```
aws ec2 create-fleet \
  --cli-input-json file://config.json
```

Pour plus d'informations, consultez [Créer une flotte EC2](#).

Exécution

La stratégie d'allocation détermine que la capacité à la demande est toujours assurée, tandis que l'équilibre de la capacité cible est assuré sous la forme d'instances spot si la capacité et la disponibilité nécessaires sont assurées.

Didacticiel : Lancer des instances à la demande en utilisant les réservations de capacité ciblées

Ce didacticiel vous guide à travers toutes les étapes que vous devez effectuer pour que votre flotte EC2 lance des instances à la demande dans les réservations de capacité `targeted`.

Vous verrez qu'il est possible de configurer une flotte EC2 pour qu'elle utilise d'abord la réservations de capacité `targeted` lors du lancement d'instances à la demande. Vous apprendrez également à configurer la flotte de sorte que, lorsque la capacité cible totale à la demande dépasse le nombre de réservations de capacité inutilisées disponibles, la flotte utilise la stratégie d'allocation spécifiée pour sélectionner les groupes d'instances dans lesquels lancer la capacité cible restante.

Configuration de la flotte EC2

Dans ce didacticiel, la configuration de la flotte est la suivante :

- Capacité cible : 10 instances à la demande
- Total de réservations de capacité `targeted` non utilisé : 6 (inférieur à la capacité cible à la demande de la flotte de 10 instances à la demande)
- Nombre de groupes de réservations de capacité : 2 (`us-east-1a` et `us-east-1b`)
- Nombre de réservations de capacité par groupe : 3
- Stratégie d'allocation à la demande : `lowest-price` (Lorsque le nombre de réservations de capacité inutilisées est inférieur à la capacité cible à la demande, la flotte détermine les groupes dans lesquels lancer la capacité à la demande restante en fonction de la stratégie d'allocation à la demande.)

Notez que vous pouvez également utiliser la stratégie d'allocation `prioritized` au lieu de la stratégie d'allocation `lowest-price`.

Pour lancer des instances à la demande dans les réservations de capacité `targeted`, vous devez effectuer un certain nombre d'étapes, comme suit :

- [Étape 1 : Créer des réservations de capacité](#)
- [Étape 2 : Création d'un groupe de ressources de Réserve de capacité](#)
- [Étape 3 : Ajouter les réservations de capacité au groupe de ressources de Réserve de capacité](#)
- [\(Facultatif\) Étape 4 : Afficher les réservations de capacité dans le groupe de ressources](#)
- [Étape 5 : Créer un modèle de lancement qui spécifie que la réservation de capacité cible un groupe de ressources spécifique](#)
- [\(Facultatif\) Étape 6 : Décrire le modèle de lancement](#)
- [Étape 7 : Créer une flotte EC2](#)
- [\(Facultatif\) Étape 8 : Afficher le nombre de réservations de capacité non utilisées restantes](#)

Étape 1 : Créer des réservations de capacité

Utilisation de la commande [create-reservation-capacity](#) (créer une réservation de capacité) pour créer les réservations de capacité, trois pour `us-east-1a` et trois autres pour `us-east-1b`. À l'exception de la zone de disponibilité, les autres attributs des réservations de capacité sont identiques.

3 Capacity Reservations in **us-east-1a** (3 réservations de capacité sur).

```
aws ec2 create-capacity-reservation \  
  --availability-zone us-east-1a\  
  --instance-type c5.xlarge\  
  --instance-platform Linux/UNIX \  
  --instance-count 3 \  
  --instance-match-criteria targeted
```

Exemple d'ID de réservation de capacité en résultant

```
cr-1234567890abcdef1
```

3 Capacity Reservations in **us-east-1b** (3 réservations de capacité sur).

```
aws ec2 create-capacity-reservation \  
  --availability-zone us-east-1b\  
  --instance-type c5.xlarge\  
  --instance-match-criteria targeted
```

```
--instance-platform Linux/UNIX \  
--instance-count 3 \  
--instance-match-criteria targeted
```

Exemple d'ID de réservation de capacité en résultant

```
cr-54321abcdef567890
```

Étape 2 : Création d'un groupe de ressources de Réserve de capacité

Utilisation de `resource-groups` et du service [create-group](#) (créer un groupe) pour créer un groupe de ressources de Réserve de capacité. Dans cet exemple, le groupe de ressources est nommé `my-cr-group`. Pour plus d'informations sur les raisons pour lesquelles vous devez créer un groupe de ressources, veuillez consulter [Utiliser réservations de capacité pour instances à la demande](#).

```
aws resource-groups create-group \  
  --name my-cr-group \  
  --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'  
'{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-  
types", "Values": ["AWS::EC2::CapacityReservation"]}]]'
```

Étape 3 : Ajouter les réservations de capacité au groupe de ressources de Réserve de capacité

Utilisation de `resource-groups` et du service [group-resources](#) (groupement de ressources) pour ajouter les réservations de capacité créées à l'étape 1 au groupe de ressources de réservations de capacité. Notez que vous devez référencer les réservations de capacité à la demande par leurs ARN.

```
aws resource-groups group-resources \  
  --group my-cr-group \  
  --resource-arns \  
    arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \  
    arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Exemple de sortie

```
{  
  "Failed": [],  
  "Succeeded": [  
    {  
      "Group": "my-cr-group",  
      "Resource": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation:cr-1234567890abcdef1",  
      "Status": "SUCCEEDED"  
    },  
    {  
      "Group": "my-cr-group",  
      "Resource": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation:cr-54321abcdef567890",  
      "Status": "SUCCEEDED"  
    }  
  ]  
}
```

```
"arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",  
"arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"  
]  
}
```

(Facultatif) Étape 4 : Afficher les réservations de capacité dans le groupe de ressources

Utilisez le `resource-groups` et le service [list-group-resources](#) (Listes-groupe-ressources) pour éventuellement décrire le groupe de ressources et afficher ses réservations de capacité.

```
aws resource-groups list-group-resources --group my-cr-group
```

Exemple de sortie

```
{  
  "ResourceIdentifiers": [  
    {  
      "ResourceType": "AWS::EC2::CapacityReservation",  
      "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/  
cr-1234567890abcdef1"  
    },  
    {  
      "ResourceType": "AWS::EC2::CapacityReservation",  
      "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/  
cr-54321abcdef567890"  
    }  
  ]  
}
```

Étape 5 : Créer un modèle de lancement qui spécifie que la réservation de capacité cible un groupe de ressources spécifique

Utilisation de la commande [create-launch-template](#) (créer un modèle de lancement) pour créer un modèle de lancement dans lequel spécifier les réservations de capacité à utiliser. Dans cet exemple, la flotte utilisera les réservations de capacité `targeted`, qui ont été ajoutées à un groupe de ressources. Par conséquent, les données du modèle de lancement spécifient que la réservation de capacité cible un groupe de ressources spécifique. Dans cet exemple, le modèle de lancement est nommé `my-launch-template`.

```
aws ec2 create-launch-template \  
  --launch-template-name my-launch-template \  
  --launch-template-data \  
    '{"ImageId": "ami-0123456789example",  
     "CapacityReservationSpecification":  
       {"CapacityReservationTarget":  
         { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-  
east-1:123456789012:group/my-cr-group" }  
       }  
     }'
```

(Facultatif) Étape 6 : Décrire le modèle de lancement

Utilisez la commande [describe-launch-template](#) (décrire le modèle de lancement) pour éventuellement décrire le modèle de lancement et afficher sa configuration.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Exemple de sortie

```
{  
  "LaunchTemplateVersions": [  
    {  
      "LaunchTemplateId": "lt-01234567890example",  
      "LaunchTemplateName": "my-launch-template",  
      "VersionNumber": 1,  
      "CreateTime": "2021-01-19T20:50:19.000Z",  
      "CreatedBy": "arn:aws:iam::123456789012:user/Admin",  
      "DefaultVersion": true,  
      "LaunchTemplateData": {  
        "ImageId": "ami-0947d2ba12ee1ff75",  
        "CapacityReservationSpecification": {  
          "CapacityReservationTarget": {  
            "CapacityReservationResourceGroupArn": "arn:aws:resource-  
groups:us-east-1:123456789012:group/my-cr-group"  
          }  
        }  
      }  
    }  
  ]  
}
```

Étape 7 : Créer une flotte EC2

Créez une flotte EC2 qui spécifie les informations de configuration pour les instances qu'il lancera. La configuration de flotte EC2 suivante affiche uniquement les configurations pertinentes pour cet exemple. Le modèle de lancement `my-launch-template` est le modèle de lancement que vous avez créé à l'étape 5. Il existe deux groupes d'instances, chacun ayant le même type d'instance (`c5.xlarge`), mais avec des zones de disponibilité différentes (`us-east-1a` et `us-east-1b`). Le prix des groupes d'instances est le même car la tarification est définie pour la Région et non pour la zone de disponibilité. La capacité cible totale est 10 et le type de capacité cible par défaut est `on-demand`. La stratégie d'allocation à la demande est `lowest-price`. La stratégie d'utilisation des réservations de capacité est `use-capacity-reservations-first`.

Note

Le type de flotte doit être `instant`. Les autres types de flotte ne prennent pas en charge `use-capacity-reservations-first`.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "my-launch-template",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "c5.xlarge",
          "AvailabilityZone": "us-east-1a"
        },
        {
          "InstanceType": "c5.xlarge",
          "AvailabilityZone": "us-east-1b"
        }
      ]
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 10,
    "DefaultTargetCapacityType": "on-demand"
  },
}
```

```
"OnDemandOptions": {
  "AllocationStrategy": "lowest-price",
  "CapacityReservationOptions": {
    "UsageStrategy": "use-capacity-reservations-first"
  }
},
>Type": "instant"
}
```

Après avoir créé la flotte `instant` à l'aide de la configuration précédente, les 10 instances suivantes sont lancées pour atteindre la capacité cible :

- Les réservations de capacité sont utilisées en premier lieu pour lancer 6 instances à la demande comme suit :
 - 3 instances à la demande sont lancées dans les 3 réservations de capacité `c5.xlarge` `targeted` dans `us-east-1a`
 - 3 instances à la demande sont lancées dans les 3 réservations de capacité `c5.xlarge` `targeted` dans `us-east-1b`
- Pour atteindre la capacité cible, 4 instances à la demande supplémentaires sont lancées dans la capacité à la demande régulière selon la stratégie d'allocation à la demande, qui est `lowest-price` dans cet exemple. Toutefois, étant donné que les groupes ont le même prix (car le prix est défini par Région et non par zone de disponibilité), la flotte lance les 4 instances à la demande restantes dans l'un ou l'autre des groupes.

(Facultatif) Étape 8 : Afficher le nombre de réservations de capacité non utilisées restantes

Une fois la flotte lancée, vous pouvez exécuter [describe-capacity-reservations](#) (décrire les réservations de capacité) pour voir combien il reste de réservations de capacité inutilisées. Dans cet exemple, vous devriez voir la réponse suivante, qui montre que tous les réservations de capacité de tous les groupes ont été utilisés.

```
{ "CapacityReservationId": "cr-111",
  "InstanceType": "c5.xlarge",
  "AvailableInstanceCount": 0
}

{ "CapacityReservationId": "cr-222",
  "InstanceType": "c5.xlarge",
```

```
"AvailableInstanceCount": 0  
}
```

Tutoriel : Lancer des instances dans des blocs de capacité

Ce didacticiel vous guide à travers les étapes que vous devez effectuer pour que votre flotte d'EC2 lance des instances à la demande dans des blocs de capacité. Pour plus d'informations sur les blocs de capacité, consultez [Blocs de capacité pour ML](#).

Vous pouvez utiliser la flotte d'EC2 de type instantané pour lancer des instances dans des blocs de capacité. Pour plus d'informations, consultez [Utilisez une flotte EC2 de type 'instantané'](#).

Dans la plupart des cas, la capacité cible de la demande de flotte d'EC2 doit être inférieure ou égale à la capacité disponible de la réservation du bloc de capacité que vous ciblez. Les demandes de capacité cible qui dépassent les limites de la réservation du bloc de capacité ne seront pas satisfaites. Si la demande de capacité cible dépasse les limites de votre réservation de bloc de capacité, vous recevrez une exception de capacité insuffisante pour la capacité qui dépasse les limites de votre réservation de bloc de capacité.

Note

Pour les blocs de capacité, les flottes d'EC2 ne se contenteront pas de lancer des instances à la demande pour le reste de la capacité cible souhaitée.

Si les flottes d'EC2 ne sont pas en mesure d'atteindre la capacité cible demandée dans une réservation de bloc de capacité disponible, les flottes d'EC2 atteindront la capacité maximale et renverront les instances qu'elles ont pu lancer. Vous pouvez répéter l'appel aux flottes d'EC2 jusqu'à ce que toutes les instances soient mises en service.

Après avoir configuré la demande de flottes d'EC2, vous devez attendre la date de début de votre réservation de bloc de capacité. Si vous demandez à aux flottes d'EC2 de se lancer dans un bloc de capacité qui n'a pas encore démarré, vous recevrez une erreur de capacité insuffisante.

Une fois que votre réservation de bloc de capacité est active, vous pouvez appeler l'API de flotte d'EC2 et mettre en service les instances dans votre bloc de capacité en fonction des paramètres que vous avez sélectionnés. Les instances exécutées dans le bloc de capacité continuent de s'exécuter jusqu'à ce que vous les arrêtiez ou les résilieez par le biais d'un appel d'API Amazon EC2 distinct ou

jusqu'à ce qu'Amazon EC2 mette fin aux instances lorsque la réservation de bloc de capacité prend fin.

Considérations

- Il est impossible de prendre en charge plusieurs blocs de capacité dans la même demande `CreateFleet`.
- L'utilisation de `OnDemandTargetCapacity` ou `SpotTargetCapacity` lors de la configuration de `capacity-block` en tant que `DefaultTargetCapacity` n'est pas prise en charge.
- Si `DefaultTargetCapacityType` est défini sur `capacity-block`, vous ne pouvez pas mettre en service `OnDemandOptions::CapacityReservationOptions`. Une exception se produit.

Création d'un modèle de lancement

L'ID de modèle de lancement est utilisé à l'étape suivante. Pour plus d'informations, consultez [Création d'un modèle de lancement](#).

Pour configurer le modèle de lancement, pour `InstanceMarketOptionsRequest`, définissez `MarketType` sur `capacity-block`. Spécifiez l'ID de réservation de bloc de capacité que vous ciblez en définissant le paramètre `CapacityReservationID`.

Créer la flotte EC2

Créez un fichier, `config.json`, avec la configuration suivante pour sa flotte d'EC2. Dans l'exemple suivant, remplacez les identificateurs de ressources par vos propres identificateurs de ressources.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "CBR-launch-template",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "p5.48xlarge",
          "AvailabilityZone": "us-east-1a"
        }
      ]
    }
  ]
}
```

```
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 10,
    "DefaultTargetCapacityType": "capacity-block"
  },
  "Type": "instant"
}
```

Utilisez la commande [create-fleet](#) suivante.

```
aws ec2 create-fleet \
  --cli-input-json file://config.json
```

Pour plus d'informations, consultez [Créer une flotte EC2](#).

Didacticiel : utiliser un flotte d'instances EC2 avec pondération des instances

Cette procédure utilise une société fictive nommée Example Corp pour illustrer le processus de demande d'une flotte d'instances EC2 utilisant la pondération des instances.

Objectif

Example Corp est une entreprise pharmaceutique qui souhaite utiliser la puissance de calcul d'Amazon EC2 pour contrôler les composants chimiques susceptibles d'être utilisés afin de lutter contre le cancer.

Planification

Example Corp commence par examiner les [bonnes pratiques en matière d'instances Spot](#). Ensuite, Example Corp détermine les exigences suivantes pour son parc d'instances Spot.

Types d'instance

Example Corp a une application qui exige beaucoup de calculs et de mémoire. Pour un fonctionnement optimal, cette application a besoin d'au moins 60 Go de mémoire et de huit UC virtuelles (vCPU). L'entreprise souhaite optimiser ces ressources pour l'application au prix le plus bas possible. Example Corp décide que l'un des types d'instance EC2 suivants est capable de répondre à ses besoins :

Type d'instance	Mémoire (Go)	vCPU
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacité cible en unités

Avec la pondération des instances, la capacité cible peut être égale à un certain nombre d'instances (valeur par défaut) ou à une combinaison de facteurs tels que les cœurs (vCPU), la mémoire GiBs () et le stockage (Go). En considérant que la base de son application (60 Go de RAM et huit vCPU) compte pour 1 unité, Example Corp décide que 20 fois cette quantité suffirait pour répondre à ses besoins. L'entreprise définit donc la capacité cible de sa demande de parc d'instances Spot sur 20.

Pondérations d'instance

Après avoir déterminé sa capacité cible, Example Corp calcule ses pondérations d'instance. Pour calculer la pondération de chaque type d'instance, l'entreprise détermine les unités de chaque type d'instance nécessaires pour atteindre la capacité cible de la façon suivante :

- r3.2xlarge (61,0 Go, 8 vCPU) = 1 unité de 20
- r3.4xlarge (122,0 Go, 16 vCPU) = 2 unités de 20
- r3.8xlarge (244,0 Go, 32 vCPU) = 4 unités de 20

Par conséquent, Example Corp assigne des pondérations d'instance de 1, 2 et 4 aux configurations de lancement respectives dans sa demande de parc d'instances Spot .

Prix par heure d'unité

Example Corp utilise le [prix à la Demande](#) par heure d'instance comme point de départ de son prix. Elle peut également utiliser les prix Spot récents ou une combinaison des deux. Pour calculer le prix par heure d'unité, elle divise le prix de départ basé sur l'heure d'instance par la pondération. Exemples :

Type d'instance	Prix à la Demande	Pondération de l'instance	Prix par heure d'unité
r3.2xLarge	0,7 USD	1	0,7 USD
r3.4xLarge	1,4 USD	2	0,7 USD
r3.8xLarge	2.8 USD	4	0,7 USD

Example Corp peut utiliser un prix global par heure d'unité s'élevant à 0,7 USD et rester concurrentielle pour les trois types d'instance. Elle peut également utiliser un prix global par heure d'unité s'élevant à 0,7 USD et un prix spécifique par heure d'unité de 0,9 USD dans la spécification de lancement du type d'instance `r3.8xlarge`.

Vérifier les autorisations

Avant de créer une demande de parc d'instances Spot, Example Corp vérifie qu'elle dispose d'un rôle IAM avec les autorisations requises. Pour plus d'informations, consultez [Autorisations du parc d'instances Spot](#).

Créer la demande

Example Corp crée un fichier, `config.json`, avec la configuration suivante pour sa demande de parc d'instances Spot :

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.2xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 1
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.4xlarge",
      "SubnetId": "subnet-482e4972",
```

```
    "WeightedCapacity": 2
  },
  {
    "ImageId": "ami-1a2b3c4d",
    "InstanceType": "r3.8xlarge",
    "SubnetId": "subnet-482e4972",
    "SpotPrice": "0.90",
    "WeightedCapacity": 4
  }
]
```

Exemple Corp crée la demande de parc d'instances Spot à l'aide de la commande [request-spot-fleet](#).

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Pour plus d'informations, consultez [Types de demande de parc d'instances Spot](#).

Exécution

La stratégie d'allocation détermine de quels groupes de capacités Spot sont issues vos instances Spot.

Avec la stratégie `lowestPrice` (qui est la stratégie par défaut), les Instances Spot sont issues du groupe ayant le prix par unité le plus bas au moment de l'exécution. Pour fournir 20 unités de capacité, le parc d'instances Spot lance 20 instances `r3.2xlarge` (20 divisé par 1), 10 instances `r3.4xlarge` (20 divisé par 2) ou 5 instances `r3.8xlarge` (20 divisé par 4).

Si Example Corp avait utilisé la stratégie `diversified`, les Instances Spot auraient été issues des trois groupes. Le parc d'instances Spot aurait lancé 6 instances `r3.2xlarge` (soit 6 unités), 3 instances `r3.4xlarge` (soit 6 unités) et 2 instances `r3.8xlarge` (soit 8 unités), pour un total de 20 unités.

Exemples de configurations pour les flottes d'instances EC2 et Spot

Les exemples suivants montrent les configurations de lancement que vous pouvez utiliser pour créer des flottes d'instances EC2 et Spot.

Rubriques

- [Exemples de configuration d'une flotte EC2](#)

- [Exemples de configuration d'un parc d'instances Spot](#)

Exemples de configuration d'une flotte EC2

Les exemples suivants montrent les configurations de lancement que vous pouvez utiliser avec la commande [create-fleet](#) pour créer une Flotte EC2. Pour plus d'informations sur les paramètres, veuillez consulter [create-fleet](#) dans la Référence des commandes AWS CLI .

Exemples

- [Exemple 1 : Lancer instances Spot en tant qu'option d'achat par défaut](#)
- [Exemple 2 : Lancer instances à la demande en tant qu'option d'achat par défaut](#)
- [Exemple 3 : Lancer instances à la demande en tant que capacité principale](#)
- [Exemple 4 : Lancer des instances à la demande à l'aide de plusieurs réservations de capacité](#)
- [Exemple 5 : Lancer des instances à la demande à l'aide de réservations de capacité lorsque la capacité cible totale dépasse le nombre de réservations de capacité non utilisées](#)
- [Exemple 6 : Lancer des instances à la demande à l'aide de réservations de capacité ciblées](#)
- [Exemple 7 : configurer le rééquilibrage de capacité pour lancer des instances Spot de remplacement](#)
- [Exemple 8 : Lancer des instances ponctuelles dans un parc à capacité optimisée](#)
- [Exemple 9 : Lancer des instances ponctuelles dans un parc à capacité optimisée avec des priorités](#)
- [Exemple 10 : Lancer des instances ponctuelles dans une price-capacity-optimized flotte](#)
- [Exemple 11 : Configuration de la sélection du type d'instance basée sur les attributs](#)

Exemple 1 : Lancer instances Spot en tant qu'option d'achat par défaut

L'exemple suivant spécifie les paramètres minimum requis dans une flotte EC2 : un modèle de lancement, une capacité cible et une option d'achat par défaut. Le modèle de lancement est identifié par son ID de modèle de lancement et son numéro de version. La capacité cible du parc d'instances est de 2 instances et l'option d'achat par défaut est spot, ce qui entraîne le lancement par le parc d'instances de 2 Instances Spot.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
```

```
        "LaunchTemplateId": "lt-0e8c754449b27161c",
        "Version": "1"
    }
},
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 2,
    "DefaultTargetCapacityType": "spot"
}
}
```

Exemple 2 : Lancer instances à la demande en tant qu'option d'achat par défaut

L'exemple suivant spécifie les paramètres minimum requis dans une flotte EC2 : un modèle de lancement, une capacité cible et une option d'achat par défaut. Le modèle de lancement est identifié par son ID de modèle de lancement et son numéro de version. La capacité cible du parc d'instances est de 2 instances et l'option d'achat par défaut est on-demand, ce qui entraîne le lancement par le parc d'instances de 2 instances à la demande.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0e8c754449b27161c",
        "Version": "1"
      }
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 2,
    "DefaultTargetCapacityType": "on-demand"
  }
}
```

Exemple 3 : Lancer instances à la demande en tant que capacité principale

L'exemple suivant spécifie la capacité cible totale de 2 instances pour la flotte d'instances et une capacité cible de 1 instance à la demande. L'option d'achat par défaut est spot. Le flotte d'instances lance 1 instance à la demande comme spécifié, mais a besoin de lancer une instance supplémentaire

pour assurer la capacité cible totale. L'option d'achat pour la différence est calculée comme $\text{TotalTargetCapacity} - \text{OnDemandTargetCapacity} = \text{DefaultTargetCapacityType}$, ce qui entraîne le lancement d'1 instance Spot par la flotte.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0e8c754449b27161c",
        "Version": "1"
      }
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 2,
    "OnDemandTargetCapacity": 1,
    "DefaultTargetCapacityType": "spot"
  }
}
```

Exemple 4 : Lancer des instances à la demande à l'aide de plusieurs réservations de capacité

Vous pouvez configurer une flotte pour qu'elle utilise d'abord Réservations de capacité à la demande lors du lancement d'Instances à la demande en définissant la stratégie d'utilisation des réservations de capacité sur `use-capacity-reservations-first`. Cet exemple montre comment la flotte sélectionne les réservations de capacité à utiliser lorsqu'il y a plus de réservations de capacité que nécessaire pour atteindre la capacité cible.

Dans cet exemple, la configuration de la flotte est la suivante :

- Capacité cible : 12 instances à la demande
- Total de réservations de capacité non utilisé : 15 (supérieur à la capacité cible à la demande de la flotte de 12 instances à la demande)
- Nombre de groupes de réservations de capacité : 3 (`m5.large`, `m4.xlarge`, et `m4.2xlarge`)
- Nombre de réservations de capacité par groupe : 5

- Stratégie d'allocation à la demande : `lowest-price` (Lorsqu'il y a plusieurs réservations de capacité inutilisées dans plusieurs groupes d'instances, la flotte détermine les groupes dans lesquels lancer les instances à la demande en fonction de la stratégie d'allocation à la demande.)

Notez que vous pouvez également utiliser la stratégie d'allocation `prioritized` au lieu de la stratégie d'allocation `lowest-price`.

Réserve de capacité

Le compte a les 15 réservations de capacité suivants inutilisés dans 3 groupes différents. Le nombre de Réservations de capacité dans chaque pool est indiqué par `AvailableInstanceCount`.

```
{
  "CapacityReservationId": "cr-111",
  "InstanceType": "m5.large",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1a",
  "AvailableInstanceCount": 5,
  "InstanceMatchCriteria": "open",
  "State": "active"
}

{
  "CapacityReservationId": "cr-222",
  "InstanceType": "m4.xlarge",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1a",
  "AvailableInstanceCount": 5,
  "InstanceMatchCriteria": "open",
  "State": "active"
}

{
  "CapacityReservationId": "cr-333",
  "InstanceType": "m4.2xlarge",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1a",
  "AvailableInstanceCount":5,
  "InstanceMatchCriteria": "open",
  "State": "active"
}
```

Fleet configuration (Configuration de la flotte)

La configuration de flotte suivante affiche uniquement les configurations pertinentes pour cet exemple. La capacité totale cible est 12 et le type de capacité cible par défaut est on-demand. La stratégie d'allocation à la demande est `lowest-price`. La stratégie d'utilisation des réservations de capacité est `use-capacity-reservations-first`.

Dans cet exemple, le prix des instance à la demande est :

- `m5.large` – 0,096 dollars par heure
- `m4.xlarge` – 0,20 dollars par heure
- `m4.2xlarge` – 0,40 dollars par heure

Note

Le type de flotte doit être `instant`. Les autres types de flotte ne prennent pas en charge `use-capacity-reservations-first`.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-abc1234567example",
        "Version": "1"
      }
      "Overrides": [
        {
          "InstanceType": "m5.large",
          "AvailabilityZone": "us-east-1a",
          "WeightedCapacity": 1
        },
        {
          "InstanceType": "m4.xlarge",
          "AvailabilityZone": "us-east-1a",
          "WeightedCapacity": 1
        },
        {
          "InstanceType": "m4.2xlarge",
          "AvailabilityZone": "us-east-1a",

```

```
        "WeightedCapacity": 1
      }
    ]
  }
],
"TargetCapacitySpecification": {
  "TotalTargetCapacity": 12,
  "DefaultTargetCapacityType": "on-demand"
},
"OnDemandOptions": {
  "AllocationStrategy": "lowest-price"
  "CapacityReservationOptions": {
    "UsageStrategy": "use-capacity-reservations-first"
  }
},
"Type": "instant",
}
```

Après avoir créé la flotte instant à l'aide de la configuration précédente, les 12 instances suivantes sont lancées pour atteindre la capacité cible :

- 5 instances à la demande m5.large dans us-east-1a – m5.large dans us-east-1a est le prix le plus bas, et il y a 5 réservations de capacité m5.large disponibles inutilisés
- 5 instances à la demande m4.xlarge dans us-east-1a – m4.xlarge dans us-east-1a est le prix suivant le plus bas, et il y a 5 réservations de capacité m4.xlarge disponibles inutilisés
- 2 instances à la demande m4.2xlarge dans us-east-1a – m4.2xlarge dans us-east-1a est le troisième prix le plus bas, et il y a 5 réservations de capacité m4.2xlarge disponibles inutilisés dont seulement 2 sont nécessaires pour atteindre la capacité cible

Une fois la flotte lancée, vous pouvez exécuter [describe-capacity-reservations](#) pour voir combien il reste de Réservations de capacité inutilisés. Dans cet exemple, vous devriez voir la réponse suivante, qui montre que tous les réservations de capacité m5.large et m4.xlarge ont été utilisés, avec 3 réservations de capacité m4.2xlarge restants inutilisés.

```
{
  "CapacityReservationId": "cr-111",
  "InstanceType": "m5.large",
  "AvailableInstanceCount": 0
}
```

```
{
  "CapacityReservationId": "cr-222",
  "InstanceType": "m4.xlarge",
  "AvailableInstanceCount": 0
}

{
  "CapacityReservationId": "cr-333",
  "InstanceType": "m4.2xlarge",
  "AvailableInstanceCount": 3
}
```

Exemple 5 : Lancer des instances à la demande à l'aide de réservations de capacité lorsque la capacité cible totale dépasse le nombre de réservations de capacité non utilisées

Vous pouvez configurer une flotte pour qu'elle utilise d'abord Réservations de capacité à la demande lors du lancement d'Instances à la demande en définissant la stratégie d'utilisation des réservations de capacité sur `use-capacity-reservations-first`. Cet exemple illustre comment la flotte sélectionne les groupes d'instances dans lesquels lancer des instances à la demande lorsque la capacité cible totale dépasse le nombre de réservations de capacité non utilisées disponibles.

Dans cet exemple, la configuration de la flotte est la suivante :

- Capacité cible : 16 instances à la demande
- Total de réservations de capacité non utilisé : 15 (inférieur à la capacité cible à la demande de la flotte de 16 instances à la demande)
- Nombre de groupes de réservations de capacité : 3 (m5.large, m4.xlarge, et m4.2xlarge)
- Nombre de réservations de capacité par groupe : 5
- Stratégie d'allocation à la demande : `lowest-price` (Lorsque le nombre de réservations de capacité inutilisées est inférieur à la capacité cible à la demande, la flotte détermine les groupes dans lesquels lancer la capacité à la demande restante en fonction de la stratégie d'allocation à la demande.)

Notez que vous pouvez également utiliser la stratégie d'allocation `prioritized` au lieu de la stratégie d'allocation `lowest-price`.

Réserve de capacité

Le compte a les 15 réservations de capacité suivants inutilisés dans 3 groupes différents. Le nombre de Réservations de capacité dans chaque pool est indiqué par `AvailableInstanceCount`.

```
{
  "CapacityReservationId": "cr-111",
  "InstanceType": "m5.large",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1a",
  "AvailableInstanceCount": 5,
  "InstanceMatchCriteria": "open",
  "State": "active"
}

{
  "CapacityReservationId": "cr-222",
  "InstanceType": "m4.xlarge",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1a",
  "AvailableInstanceCount": 5,
  "InstanceMatchCriteria": "open",
  "State": "active"
}

{
  "CapacityReservationId": "cr-333",
  "InstanceType": "m4.2xlarge",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1a",
  "AvailableInstanceCount": 5,
  "InstanceMatchCriteria": "open",
  "State": "active"
}
```

Fleet configuration (Configuration de la flotte)

La configuration de flotte suivante affiche uniquement les configurations pertinentes pour cet exemple. La capacité cible totale est 16 et le type de capacité cible par défaut est on-demand. La stratégie d'allocation à la demande est `lowest-price`. La stratégie d'utilisation des réservations de capacité est `use-capacity-reservations-first`.

Dans cet exemple, le prix des instance à la demande est :

- m5.large – 0,096 USD par heure
- m4.xlarge – 0,20 USD par heure
- m4.2xlarge – 0,40 USD par heure

 Note

Le type de flotte doit être instant. Les autres types de flotte ne prennent pas en charge `use-capacity-reservations-first`.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0e8c754449b27161c",
        "Version": "1"
      }
      "Overrides": [
        {
          "InstanceType": "m5.large",
          "AvailabilityZone": "us-east-1a",
          "WeightedCapacity": 1
        },
        {
          "InstanceType": "m4.xlarge",
          "AvailabilityZone": "us-east-1a",
          "WeightedCapacity": 1
        },
        {
          "InstanceType": "m4.2xlarge",
          "AvailabilityZone": "us-east-1a",
          "WeightedCapacity": 1
        }
      ]
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 16,
```

```
    "DefaultTargetCapacityType": "on-demand"
  },
  "OnDemandOptions": {
    "AllocationStrategy": "lowest-price"
    "CapacityReservationOptions": {
      "UsageStrategy": "use-capacity-reservations-first"
    }
  },
  "Type": "instant",
}
```

Après avoir créé la flotte instant à l'aide de la configuration précédente, les 16 instances suivantes sont lancées pour atteindre la capacité cible :

- 6 instances à la demande m5.large dans us-east-1a – m5.large dans us-east-1a est le prix le plus bas, et il y a 5 réservations de capacité m5.large disponibles inutilisés Les réservations de capacité sont utilisées en premier afin de lancer 5 instances à la demande. Après l'utilisation des réservations de capacité m4.xlarge and m4.2xlarge restantes, une instance à la demande supplémentaire est lancée pour atteindre la capacité cible, conformément à la stratégie d'allocation à la demande, qui est lowest-price dans cet exemple.
- 5 instances à la demande m4.xlarge dans us-east-1a – m4.xlarge dans us-east-1a est le prix suivant le plus bas, et il y a 5 réservations de capacité m4.xlarge disponibles inutilisés
- 5 instances à la demande m4.2xlarge dans us-east-1a – m4.2xlarge dans us-east-1a est le troisième prix le plus bas, et il y a 5 réservations de capacité m4.2xlarge disponibles inutilisés

Une fois la flotte lancée, vous pouvez exécuter [describe-capacity-reservations](#) pour voir combien il reste de Réservations de capacité inutilisés. Dans cet exemple, vous devriez voir la réponse suivante, qui montre que tous les Réservations de capacité de tous les groupes ont été utilisés.

```
{
  "CapacityReservationId": "cr-111",
  "InstanceType": "m5.large",
  "AvailableInstanceCount": 0
}

{
  "CapacityReservationId": "cr-222",
  "InstanceType": "m4.xlarge",
  "AvailableInstanceCount": 0
}
```

```
{
  "CapacityReservationId": "cr-333",
  "InstanceType": "m4.2xlarge",
  "AvailableInstanceCount": 0
}
```

Exemple 6 : Lancer des instances à la demande à l'aide de réservations de capacité ciblées

Vous pouvez configurer une flotte pour qu'elle utilise `targeted` d'abord les réservations de capacité à la demande lors du lancement d'instances à la demande en paramétrant la stratégie d'utilisation des réservations de capacité sur `use-capacity-reservations-first`. Cet exemple illustre comment lancer des instances à la demande dans réservations de capacité `targeted`, où les attributs des réservations de capacité sont les mêmes, à l'exception de leurs zones de disponibilité (`us-east-1a` et `us-east-1b`). Il illustre également comment la flotte sélectionne les groupes d'instances dans lesquels lancer des instances à la demande lorsque la capacité cible totale dépasse le nombre de réservations de capacité non utilisées disponibles.

Dans cet exemple, la configuration de la flotte est la suivante :

- Capacité cible : 10 instances à la demande
- Total de réservations de capacité `targeted` non utilisé : 6 (inférieur à la capacité cible à la demande de la flotte de 10 instances à la demande)
- Nombre de groupes de réservations de capacité : 2 (`us-east-1a` et `us-east-1b`)
- Nombre de réservations de capacité par groupe : 3
- Stratégie d'allocation à la demande : `lowest-price` (Lorsque le nombre de réservations de capacité inutilisées est inférieur à la capacité cible à la demande, la flotte détermine les groupes dans lesquels lancer la capacité à la demande restante en fonction de la stratégie d'allocation à la demande.)

Notez que vous pouvez également utiliser la stratégie d'allocation `prioritized` au lieu de la stratégie d'allocation `lowest-price`.

Pour obtenir une démonstration pas à pas des procédures que vous devez effectuer pour exécuter cet exemple, veuillez consulter [Didacticiel : Lancer des instances à la demande en utilisant les réservations de capacité ciblées](#).

Réserve de capacité

Le compte a les 6 réservations de capacité suivants inutilisés dans 2 groupes différents. Dans cet exemple, les groupes diffèrent selon leurs zones de disponibilité. Le nombre de Réservations de capacité dans chaque pool est indiqué par `AvailableInstanceCount`.

```
{
  "CapacityReservationId": "cr-111",
  "InstanceType": "c5.xlarge",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1a",
  "AvailableInstanceCount": 3,
  "InstanceMatchCriteria": "open",
  "State": "active"
}

{
  "CapacityReservationId": "cr-222",
  "InstanceType": "c5.xlarge",
  "InstancePlatform": "Linux/UNIX",
  "AvailabilityZone": "us-east-1b",
  "AvailableInstanceCount": 3,
  "InstanceMatchCriteria": "open",
  "State": "active"
}
```

Fleet configuration (Configuration de la flotte)

La configuration de flotte suivante affiche uniquement les configurations pertinentes pour cet exemple. La capacité cible totale est 10 et le type de capacité cible par défaut est `on-demand`. La stratégie d'allocation à la demande est `lowest-price`. La stratégie d'utilisation des réservations de capacité est `use-capacity-reservations-first`.

Dans cet exemple, le prix des instance à la demande pour `c5.xlarge` dans `us-east-1` est 0,17 dollars par heure.

Note

Le type de flotte doit être `instant`. Les autres types de flotte ne prennent pas en charge `use-capacity-reservations-first`.

```
{
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "my-launch-template",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "c5.xlarge",
          "AvailabilityZone": "us-east-1a"
        },
        {
          "InstanceType": "c5.xlarge",
          "AvailabilityZone": "us-east-1b"
        }
      ]
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 10,
    "DefaultTargetCapacityType": "on-demand"
  },
  "OnDemandOptions": {
    "AllocationStrategy": "lowest-price",
    "CapacityReservationOptions": {
      "UsageStrategy": "use-capacity-reservations-first"
    }
  },
  "Type": "instant"
}
```

Après avoir créé la flotte instant à l'aide de la configuration précédente, les 10 instances suivantes sont lancées pour atteindre la capacité cible :

- Les réservations de capacité sont utilisées en premier lieu pour lancer 6 instances à la demande comme suit :
 - 3 instances à la demande sont lancées dans les 3 réservations de capacité c5.xlarge targeted dans us-east-1a
 - 3 instances à la demande sont lancées dans les 3 réservations de capacité c5.xlarge targeted dans us-east-1b

- Pour atteindre la capacité cible, 4 instances à la demande supplémentaires sont lancées dans la capacité à la demande régulière selon la stratégie d'allocation à la demande, qui est `Lowest-price` dans cet exemple. Toutefois, étant donné que les groupes ont le même prix (car le prix est défini par Région et non par zone de disponibilité), la flotte lance les 4 instances à la demande restantes dans l'un ou l'autre des groupes.

Une fois la flotte lancée, vous pouvez exécuter [describe-capacity-reservations](#) pour voir combien il reste de Réservations de capacité inutilisés. Dans cet exemple, vous devriez voir la réponse suivante, qui montre que tous les Réservations de capacité de tous les groupes ont été utilisés.

```
{
  "CapacityReservationId": "cr-111",
  "InstanceType": "c5.xlarge",
  "AvailableInstanceCount": 0
}

{
  "CapacityReservationId": "cr-222",
  "InstanceType": "c5.xlarge",
  "AvailableInstanceCount": 0
}
```

Exemple 7 : configurer le rééquilibrage de capacité pour lancer des instances Spot de remplacement

L'exemple suivant configure la flotte EC2 pour lancer une instance Spot de remplacement lorsqu'Amazon EC2 émet une recommandation de rééquilibrage pour une instance Spot dans la flotte. Pour configurer le remplacement automatique de Instances Spot, pour `ReplacementStrategy`, spécifiez `launch-before-terminate`. Pour configurer le délai entre le lancement des nouvelles instances Spot de remplacement et le moment où les anciennes instances Spot sont automatiquement supprimées, pour `termination-delay`, spécifiez une valeur en secondes. Pour plus d'informations, consultez [Options de configuration](#).

Note

Nous vous recommandons d'utiliser `launch-before-terminate` uniquement si vous pouvez prédire en combien de temps les procédures d'arrêt de vos instances seront

terminées, de sorte que les anciennes instances ne soient terminées qu'une fois ces procédures terminées. Toutes les instances en cours d'exécution vous sont facturées.

L'efficacité de la stratégie de rééquilibrage de capacité dépend du nombre de groupes de capacités Spot spécifiés dans la demande de flotte EC2. Nous vous recommandons de configurer le parc avec un ensemble diversifié de types d'instance et de zones de disponibilité, et pour `AllocationStrategy`, spécifiez `capacity-optimized`. Pour plus d'informations sur ce que vous devez prendre en compte lors de la configuration d'une Flotte EC2 pour le rééquilibrage de capacité, reportez-vous à la section [Rééquilibrage de la capacité](#).

```
{
  "ExcessCapacityTerminationPolicy": "termination",
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "LaunchTemplate",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "c3.large",
          "WeightedCapacity": 1,
          "Placement": {
            "AvailabilityZone": "us-east-1a"
          }
        },
        {
          "InstanceType": "c4.large",
          "WeightedCapacity": 1,
          "Placement": {
            "AvailabilityZone": "us-east-1a"
          }
        },
        {
          "InstanceType": "c5.large",
          "WeightedCapacity": 1,
          "Placement": {
            "AvailabilityZone": "us-east-1a"
          }
        }
      ]
    }
  ]
}
```

```
    }
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 5,
    "DefaultTargetCapacityType": "spot"
  },
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized",
    "MaintenanceStrategies": {
      "CapacityRebalance": {
        "ReplacementStrategy": "launch-before-terminate",
        "TerminationDelay": "720"
      }
    }
  }
}
```

Exemple 8 : Lancer des instances ponctuelles dans un parc à capacité optimisée

L'exemple suivant montre comment configurer une flotte EC2 avec une stratégie d'allocation Spot qui optimise la capacité. Pour optimiser la capacité, vous devez définir `AllocationStrategy` sur `capacity-optimized`.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. La capacité cible est de 50 instances Spot. La flotte EC2 tente de lancer 50 instances Spot dans le groupe de capacités Spot avec une capacité optimale pour le nombre d'instances qui sont lancées.

```
{
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized",
  },
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "my-launch-template",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "r4.2xlarge",
          "Placement": {
```

```
        "AvailabilityZone": "us-west-2a"
      },
    ],
    {
      "InstanceType": "m4.2xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2b"
      },
    },
    {
      "InstanceType": "c5.2xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2b"
      }
    }
  ]
},
"TargetCapacitySpecification": {
  "TotalTargetCapacity": 50,
  "DefaultTargetCapacityType": "spot"
}
}
```

Exemple 9 : Lancer des instances ponctuelles dans un parc à capacité optimisée avec des priorités

L'exemple suivant montre comment configurer une flotte EC2 avec une stratégie d'allocation Spot qui optimise la capacité tout en utilisant la priorité sur la base du meilleur effort.

Lors de l'utilisation de la stratégie d'allocation `capacity-optimized-prioritized`, vous pouvez utiliser le paramètre `Priority` pour spécifier les priorités des groupes de capacités Spot, où plus le nombre est faible, plus la priorité est élevée. Vous pouvez également définir la même priorité pour plusieurs groupes de capacités Spot si vous les privilégiez également. Si vous ne définissez pas de priorité pour un groupe, le groupe sera considéré comme le dernier en termes de priorité.

Pour hiérarchiser les groupes de capacités Spot, vous devez définir `AllocationStrategy` sur `capacity-optimized-prioritized`. La flotte EC2 optimisera d'abord la capacité, mais respectera les priorités sur la base du meilleur effort (par exemple, si le respect des priorités n'affecte pas de manière significative la capacité de la flotte EC2 à fournir une capacité optimale). C'est

une bonne option pour les charges de travail pour lesquelles la possibilité de perturbation doit être minimisée, mais la priorité de certains types d'instances est également importante.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. Chaque groupe est classé par ordre de priorité, où plus le nombre est faible, plus la priorité est élevée. La capacité cible est de 50 instances Spot. La flotte EC2 tente de lancer 50 instances Spot dans le groupe de capacités Spot avec la priorité la plus élevée sur la base du meilleur effort, mais optimise d'abord la capacité.

```
{
  "SpotOptions": {
    "AllocationStrategy": "capacity-optimized-prioritized"
  },
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "my-launch-template",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "r4.2xlarge",
          "Priority": 1,
          "Placement": {
            "AvailabilityZone": "us-west-2a"
          }
        },
        {
          "InstanceType": "m4.2xlarge",
          "Priority": 2,
          "Placement": {
            "AvailabilityZone": "us-west-2b"
          }
        },
        {
          "InstanceType": "c5.2xlarge",
          "Priority": 3,
          "Placement": {
            "AvailabilityZone": "us-west-2b"
          }
        }
      ]
    }
  ]
}
```

```
  ],
  "TargetCapacitySpecification": {
    "TotalTargetCapacity": 50,
    "DefaultTargetCapacityType": "spot"
  }
}
```

Exemple 10 : Lancer des instances ponctuelles dans une price-capacity-optimized flotte

L'exemple suivant montre comment configurer une flotte EC2 avec une stratégie d'allocation Spot qui optimise la capacité et le prix le plus bas. Pour optimiser la capacité tout en tenant compte du prix, vous devez définir le Spot AllocationStrategy sur price-capacity-optimized.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. La capacité cible est de 50 instances Spot. La flotte EC2 tente de lancer 50 instances Spot dans le groupe de capacités Spot avec une capacité optimale pour le nombre d'instances qui sont lancées, tout en choisissant également le groupe le moins cher.

```
{
  "SpotOptions": {
    "AllocationStrategy": "price-capacity-optimized",
    "MinTargetCapacity": 2,
    "SingleInstanceType": true
  },
  "OnDemandOptions": {
    "AllocationStrategy": "lowest-price"
  },
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "my-launch-template",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "r4.2xlarge",
          "Placement": {
            "AvailabilityZone": "us-west-2a"
          },
        },
        {
          "InstanceType": "m4.2xlarge",

```

```

        "Placement": {
            "AvailabilityZone": "us-west-2b"
        },
    },
    {
        "InstanceType": "c5.2xlarge",
        "Placement": {
            "AvailabilityZone": "us-west-2b"
        }
    }
]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 50,
    "OnDemandTargetCapacity": 0,
    "SpotTargetCapacity": 50,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}

```

Exemple 11 : Configuration de la sélection du type d'instance basée sur les attributs

L'exemple suivant montre comment configurer une flotte EC2 pour qu'elle utilise la sélection de type d'instance basée sur des attributs pour identifier les types d'instance. Pour spécifier les attributs d'instance requis, vous devez les spécifier dans la structure `InstanceRequirements`.

Dans l'exemple suivant, deux attributs d'instance sont spécifiés :

- `VCpuCount` : au moins 2 vCPU sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.
- `MemoryMiB` : au moins 4 Mio de mémoire sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.

Tout type d'instance doté d'au moins 2 vCPU et d'au moins 4 Mio de mémoire sera identifié.

Toutefois, la protection des prix et la stratégie d'allocation peuvent exclure certains types d'instances lorsque [la flotte EC2 alloue la flotte](#).

Pour obtenir une liste et une description de tous les attributs possibles que vous pouvez spécifier, consultez le [InstanceRequirements](#) manuel Amazon EC2 API Reference.

```
{
  "SpotOptions": {
    "AllocationStrategy": "price-capacity-optimized"
  },
  "LaunchTemplateConfigs": [{
    "LaunchTemplateSpecification": {
      "LaunchTemplateName": "my-launch-template",
      "Version": "1"
    },
    "Overrides": [{
      "InstanceRequirements": {
        "VCpuCount": {
          "Min": 2
        },
        "MemoryMiB": {
          "Min": 4
        }
      }
    }
  ]
},
"TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemples de configuration d'un parc d'instances Spot

Les exemples suivants montrent les configurations de lancement que vous pouvez utiliser avec la [commande request-spot-fleet](#) afin de créer une demande de parc d'instances Spot. Pour plus d'informations, consultez [Créer une Spot Fleet request](#).

Note

Pour le parc d'instances Spot, vous ne pouvez pas spécifier d'ID d'interface réseau dans un modèle ou une spécification de lancement. Veillez à omettre le paramètre `NetworkInterfaceID` dans votre modèle ou spécification de lancement.

Exemples

- [Exemple 1 : Lancement d'instances Spot en utilisant la zone de disponibilité ou le sous-réseau offrant le prix le moins élevé de la région](#)
- [Exemple 2 : Lancement d'instances Spot en utilisant la zone de disponibilité ou le sous-réseau offrant le prix le moins élevé dans une liste spécifiée](#)
- [Exemple 3 : Lancement d'instances Spot en utilisant le type d'instance offrant le prix le plus bas dans une liste spécifiée](#)
- [Exemple 4 : Remplacement du prix pour la demande](#)
- [Exemple 5 : lancement d'un parc d'instances Spot en utilisant la stratégie d'allocation diversifiée](#)
- [Exemple 6 : lancement d'un parc d'instances Spot en utilisant la pondération d'instance](#)
- [Exemple 7 : lancement d'un parc d'instances Spot avec une capacité à la demande](#)
- [Exemple 8 : Configurer le rééquilibrage de capacité pour lancer les instances Spot de remplacement](#)
- [Exemple 9 : lancer des instances Spot dans une flotte optimisée pour la capacité](#)
- [Exemple 10 : lancer des instances Spot dans une flotte optimisée pour la capacité avec des priorités](#)
- [Exemple 11 : Lancer des instances ponctuelles dans une priceCapacityOptimized flotte](#)
- [Exemple 12 : configurer la sélection de type d'instance basée sur des attributs](#)

Exemple 1 : Lancement d'instances Spot en utilisant la zone de disponibilité ou le sous-réseau offrant le prix le moins élevé de la région

L'exemple suivant spécifie une seule spécification de lancement sans Zone de disponibilité ou sous-réseau. Le parc d'instances Spot lance les instances dans la zone de disponibilité ayant le prix le moins élevé qui a un sous-réseau par défaut. Le prix que vous payez ne dépasse pas le prix à la demande.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "KeyName": "my-key-pair",
      "SecurityGroups": [
        {
```

```
        "GroupId": "sg-1a2b3c4d"
      }
    ],
    "InstanceType": "m3.medium",
    "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
    }
  }
]
}
```

Exemple 2 : Lancement d'instances Spot en utilisant la zone de disponibilité ou le sous-réseau offrant le prix le moins élevé dans une liste spécifiée

Les exemples suivants spécifient deux spécifications de lancement avec différents sous-réseaux ou zones de disponibilité, mais avec les mêmes types d'instance et AMI.

Zones de disponibilité

Le parc d'instances Spot lance les instances dans le sous-réseau par défaut de la zone de disponibilité ayant le prix le moins élevé que vous avez spécifié.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "KeyName": "my-key-pair",
      "SecurityGroups": [
        {
          "GroupId": "sg-1a2b3c4d"
        }
      ],
      "InstanceType": "m3.medium",
      "Placement": {
        "AvailabilityZone": "us-west-2a, us-west-2b"
      },
      "IamInstanceProfile": {
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
      }
    }
  ]
}
```

```
]
}
```

Sous-réseaux

Vous pouvez spécifier des sous-réseaux par défaut ou personnalisés, les derniers pouvant être issus d'un VPC par défaut ou personnalisé. Le service d'instances Spot lance les instances sur n'importe quel réseau se trouvant dans la zone de disponibilité ayant le prix le moins élevé.

Vous ne pouvez pas spécifier plusieurs sous-réseaux d'une même zone de disponibilité dans une demande de parc d'instances Spot.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "KeyName": "my-key-pair",
      "SecurityGroups": [
        {
          "GroupId": "sg-1a2b3c4d"
        }
      ],
      "InstanceType": "m3.medium",
      "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
      "IamInstanceProfile": {
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
      }
    }
  ]
}
```

Si les instances sont lancées sur un VPC par défaut, elles reçoivent une adresse IPv4 publique par défaut. Si les instances sont lancées sur un VPC personnalisé, elles ne reçoivent pas d'adresse IPv4 publique par défaut. Utilisez une interface réseau dans la spécification de lancement afin d'attribuer une adresse IPv4 publique aux instances lancées dans un VPC personnalisé. Lorsque vous spécifiez une interface réseau, vous devez inclure l'ID de sous-réseau et l'ID du groupe de sécurité à l'aide de l'interface réseau.

...

```
{
  "ImageId": "ami-1a2b3c4d",
  "KeyName": "my-key-pair",
  "InstanceType": "m3.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d",
      "Groups": [ "sg-1a2b3c4d" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
    "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"
  }
}
...

```

Exemple 3 : Lancement d'instances Spot en utilisant le type d'instance offrant le prix le plus bas dans une liste spécifiée

Les exemples suivants spécifient deux configurations de lancement avec différents types d'instance, mais la même AMI et la même zone de disponibilité ou le même sous-réseau. Le parc d'instances Spot lance les instances en utilisant le type d'instance spécifié offrant le prix le plus bas.

Zone de disponibilité

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "SecurityGroups": [
        {
          "GroupId": "sg-1a2b3c4d"
        }
      ],
      "InstanceType": "c5.4xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2b"
      }
    }
  ],
},

```

```
{
  "ImageId": "ami-1a2b3c4d",
  "SecurityGroups": [
    {
      "GroupId": "sg-1a2b3c4d"
    }
  ],
  "InstanceType": "r3.8xlarge",
  "Placement": {
    "AvailabilityZone": "us-west-2b"
  }
}
}
```

Sous-réseau

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "SecurityGroups": [
        {
          "GroupId": "sg-1a2b3c4d"
        }
      ],
      "InstanceType": "c5.4xlarge",
      "SubnetId": "subnet-1a2b3c4d"
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "SecurityGroups": [
        {
          "GroupId": "sg-1a2b3c4d"
        }
      ],
      "InstanceType": "r3.8xlarge",
      "SubnetId": "subnet-1a2b3c4d"
    }
  ]
}
```

Exemple 4 : Remplacement du prix pour la demande

Nous vous avons recommandé d'utiliser le prix maximum par défaut, qui correspond au prix à la demande. Si vous préférez, vous pouvez indiquer un prix maximum pour la demande du flotte, et les prix maximum des spécifications de lancement individuelles.

Les exemples suivants indiquent le prix maximum pour la demande du flotte, et les prix maximum pour deux des trois spécifications de lancement. Le prix maximum de la demande de flotte est utilisé pour toutes les spécifications de lancement qui ne spécifient aucun prix maximum. Le parc d'instances Spot lance les instances en utilisant le type d'instance offrant le prix le plus bas.

Zone de disponibilité

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c3.2xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2b"
      },
      "SpotPrice": "0.10"
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c3.4xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2b"
      },
      "SpotPrice": "0.20"
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c3.8xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2b"
      }
    }
  ]
}
```

```
}
```

Sous-réseau

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c3.2xlarge",
      "SubnetId": "subnet-1a2b3c4d",
      "SpotPrice": "0.10"
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c3.4xlarge",
      "SubnetId": "subnet-1a2b3c4d",
      "SpotPrice": "0.20"
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c3.8xlarge",
      "SubnetId": "subnet-1a2b3c4d"
    }
  ]
}
```

Exemple 5 : lancement d'un parc d'instances Spot en utilisant la stratégie d'allocation diversifiée

L'exemple suivant utilise la stratégie d'allocation *diversified*. Les spécifications de lancement ont différents types d'instance, mais la même AMI et la même zone de disponibilité ou le même sous-réseau. Le parc d'instances Spot répartit les 30 instances entre les trois spécifications de lancement de sorte qu'il existe 10 instances de chaque type. Pour plus d'informations, consultez [Stratégies d'allocation pour instances Spot](#).

Zone de disponibilité

```
{
```

```
"SpotPrice": "0.70",
"TargetCapacity": 30,
"AllocationStrategy": "diversified",
"IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
"LaunchSpecifications": [
  {
    "ImageId": "ami-1a2b3c4d",
    "InstanceType": "c4.2xlarge",
    "Placement": {
      "AvailabilityZone": "us-west-2b"
    }
  },
  {
    "ImageId": "ami-1a2b3c4d",
    "InstanceType": "m3.2xlarge",
    "Placement": {
      "AvailabilityZone": "us-west-2b"
    }
  },
  {
    "ImageId": "ami-1a2b3c4d",
    "InstanceType": "r3.2xlarge",
    "Placement": {
      "AvailabilityZone": "us-west-2b"
    }
  }
]
```

Sous-réseau

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c4.2xlarge",
      "SubnetId": "subnet-1a2b3c4d"
    },
    {
```

```

        "ImageId": "ami-1a2b3c4d",
        "InstanceType": "m3.2xlarge",
        "SubnetId": "subnet-1a2b3c4d"
    },
    {
        "ImageId": "ami-1a2b3c4d",
        "InstanceType": "r3.2xlarge",
        "SubnetId": "subnet-1a2b3c4d"
    }
]
}

```

Une bonne pratique pour augmenter les chances qu'une demande au comptant puisse être satisfaite par une capacité EC2 en cas de panne dans l'une des zones de disponibilité est de diversifier ces dernières. Pour ce scénario, incluez chaque zone disponibilité à votre disposition dans les spécifications de lancement. Et, au lieu d'utiliser le même sous-réseau à chaque fois, utilisez trois sous-réseaux uniques (chacun correspondant à une zone différente).

Zone de disponibilité

```

{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam:123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c4.2xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2a"
      }
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "m3.2xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2b"
      }
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.2xlarge",
    }
  ]
}

```

```
        "Placement": {
            "AvailabilityZone": "us-west-2c"
        }
    ]
}
```

Sous-réseau

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c4.2xlarge",
      "SubnetId": "subnet-1a2b3c4d"
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "m3.2xlarge",
      "SubnetId": "subnet-2a2b3c4d"
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.2xlarge",
      "SubnetId": "subnet-3a2b3c4d"
    }
  ]
}
```

Exemple 6 : lancement d'un parc d'instances Spot en utilisant la pondération d'instance

Les exemples suivants utilisent la pondération d'instance, ce qui signifie que le prix est déterminé par heure d'unité, et non par heure d'instance. Chaque configuration de lancement répertorie un type d'instance différent et une pondération différente. Le parc d'instances Spot sélectionne le type d'instance ayant le prix par heure d'unité le plus bas. Le parc d'instances Spot calcule le nombre d'instances Spot à lancer en divisant la capacité cible par la pondération d'instance. Si le résultat

n'est pas un nombre entier, le parc d'instances Spot l'arrondit à l'entier suivant afin que la taille de votre flotte ne soit pas inférieure à sa capacité cible.

Si la demande `r3.2xlarge` est satisfaite, le parc d'instances Spot met en service 4 de ces instances. Divisez 20 par 6 pour un total de 3,33 instances, puis arrondissez à 4 instances.

Si la demande `c3.xlarge` est satisfaite, le parc d'instances Spot met en service 7 de ces instances. Divisez 20 par 3 pour un total de 6,66 instances, puis arrondissez à 7 instances.

Pour plus d'informations, consultez [Pondération d'instance de parc d'instances Spot](#).

Zone de disponibilité

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.2xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2b"
      },
      "WeightedCapacity": 6
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "c3.xlarge",
      "Placement": {
        "AvailabilityZone": "us-west-2b"
      },
      "WeightedCapacity": 3
    }
  ]
}
```

Sous-réseau

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
```

```

"LaunchSpecifications": [
  {
    "ImageId": "ami-1a2b3c4d",
    "InstanceType": "r3.2xlarge",
    "SubnetId": "subnet-1a2b3c4d",
    "WeightedCapacity": 6
  },
  {
    "ImageId": "ami-1a2b3c4d",
    "InstanceType": "c3.xlarge",
    "SubnetId": "subnet-1a2b3c4d",
    "WeightedCapacity": 3
  }
]
}

```

Exemple 7 : lancement d'un parc d'instances Spot avec une capacité à la demande

Pour garantir que vous avez toujours la capacité d'instance, vous pouvez inclure une demande de capacité à la demande dans votre demande de parc d'instances Spot. S'il y a la capacité nécessaire, la demande à la demande est toujours satisfaite. Le solde de la capacité cible est assuré en tant que Spot s'il existe une capacité et une disponibilité.

L'exemple suivant spécifie la capacité cible souhaitée de 10 instances, dont 5 correspondent à une capacité à la demande. La capacité Spot n'est pas spécifiée : elle est impliquée dans le solde de la capacité cible moins la capacité à la demande. Amazon EC2 lance 5 unités de capacité à la demande et 5 unités de capacité (10 - 5 = 5) Spot s'il existe une capacité Amazon EC2 et une disponibilité.

Pour plus d'informations, consultez [À la demande dans la demande de parc d'instances Spot](#).

```

{
  "IamFleetRole": "arn:aws:iam::781603563322:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [

```

```
{
  "LaunchTemplateSpecification": {
    "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
    "Version": "2"
  },
  "Overrides": [
    {
      "InstanceType": "t2.medium",
      "WeightedCapacity": 1,
      "SubnetId": "subnet-d0dc51fb"
    }
  ]
}
```

Exemple 8 : Configurer le rééquilibrage de capacité pour lancer les instances Spot de remplacement

L'exemple suivant configure le parc d'instances Spot pour lancer une instance Spot de remplacement lorsqu'Amazon EC2 émet une recommandation de rééquilibrage pour une instance Spot de la flotte. Pour configurer le remplacement automatique de Instances Spot, pour `ReplacementStrategy`, spécifiez `launch-before-terminate`. Pour configurer le délai entre le lancement des nouvelles instances Spot de remplacement et le moment où les anciennes instances Spot sont automatiquement supprimées, pour `termination-delay`, spécifiez une valeur en secondes. Pour plus d'informations, consultez [Options de configuration](#).

Note

Nous vous recommandons d'utiliser `launch-before-terminate` uniquement si vous pouvez prédire la durée de la procédure d'arrêt de votre instance. Cela garantit que les anciennes instances ne sont résiliées qu'une fois les procédures d'arrêt terminées. Toutes les instances en cours d'exécution vous sont facturées.

L'efficacité de la stratégie de rééquilibrage de capacité dépend du nombre de groupes de capacités Spot spécifiés dans la demande de parc d'instances Spot. Nous vous recommandons de configurer le parc avec un ensemble diversifié de types d'instance et de zones de disponibilité, et pour `AllocationStrategy`, spécifiez `capacityOptimized`. Pour plus d'informations sur ce que vous

devez prendre en compte lors de la configuration d'un parc d'instances Spot pour le rééquilibrage de capacité, consultez la rubrique [Rééquilibrage de la capacité](#).

```
{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "capacityOptimized",
    "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchTemplateConfigs": [
      {
        "LaunchTemplateSpecification": {
          "LaunchTemplateName": "LaunchTemplate",
          "Version": "1"
        },
        "Overrides": [
          {
            "InstanceType": "c3.large",
            "WeightedCapacity": 1,
            "Placement": {
              "AvailabilityZone": "us-east-1a"
            }
          },
          {
            "InstanceType": "c4.large",
            "WeightedCapacity": 1,
            "Placement": {
              "AvailabilityZone": "us-east-1a"
            }
          },
          {
            "InstanceType": "c5.large",
            "WeightedCapacity": 1,
            "Placement": {
              "AvailabilityZone": "us-east-1a"
            }
          }
        ]
      }
    ],
    "TargetCapacity": 5,
    "SpotMaintenanceStrategies": {
      "CapacityRebalance": {
        "ReplacementStrategy": "launch-before-terminate",
```

```

        "TerminationDelay": "720"
    }
}
}
}

```

Exemple 9 : lancer des instances Spot dans une flotte optimisée pour la capacité

L'exemple suivant montre comment configurer un parc d'instances Spot avec une stratégie d'allocation Spot qui optimise la capacité. Pour optimiser la capacité, vous devez définir `AllocationStrategy` sur `capacityOptimized`.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. La capacité cible est de 50 instances Spot. Le parc d'instances Spot tente de lancer 50 instances Spot dans le groupe de capacités Spot avec une capacité optimale pour le nombre d'instances qui sont lancées.

```

{
  "TargetCapacity": "50",
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "capacityOptimized",
  },
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateName": "my-launch-template",
        "Version": "1"
      },
      "Overrides": [
        {
          "InstanceType": "r4.2xlarge",
          "AvailabilityZone": "us-west-2a"
        },
        {
          "InstanceType": "m4.2xlarge",
          "AvailabilityZone": "us-west-2b"
        },
        {
          "InstanceType": "c5.2xlarge",
          "AvailabilityZone": "us-west-2b"
        }
      ]
    }
  ]
}

```

```
    }  
  ]  
}
```

Exemple 10 : lancer des instances Spot dans une flotte optimisée pour la capacité avec des priorités

L'exemple suivant montre comment configurer un parc d'instances Spot avec une stratégie d'allocation Spot qui optimise la capacité tout en utilisant la priorité sur la base du meilleur effort.

Lors de l'utilisation de la stratégie d'allocation `capacityOptimizedPrioritized`, vous pouvez utiliser le paramètre `Priority` pour spécifier les priorités des groupes de capacités Spot, où plus le nombre est faible, plus la priorité est élevée. Vous pouvez également définir la même priorité pour plusieurs groupes de capacités Spot si vous les privilégiez également. Si vous ne définissez pas de priorité pour un groupe, le groupe sera considéré comme le dernier en termes de priorité.

Pour hiérarchiser les groupes de capacités Spot, vous devez définir `AllocationStrategy` sur `capacityOptimizedPrioritized`. Le parc d'instances Spot optimisera la capacité d'abord, mais respectera les priorités sur la base du meilleur effort (par exemple, si le respect des priorités n'affecte pas de manière significative la capacité du parc d'instances Spot à fournir une capacité optimale). C'est une bonne option pour les charges de travail pour lesquelles la possibilité de perturbation doit être minimisée, mais la priorité de certains types d'instances est également importante.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. Chaque groupe est classé par ordre de priorité, où plus le nombre est faible, plus la priorité est élevée. La capacité cible est de 50 instances Spot. Le parc d'instances Spot tente de lancer 50 instances Spot dans le groupe de capacités Spot avec la priorité la plus élevée sur la base du meilleur effort, mais optimise d'abord la capacité.

```
{  
  "TargetCapacity": "50",  
  "SpotFleetRequestConfig": {  
    "AllocationStrategy": "capacityOptimizedPrioritized"  
  },  
  "LaunchTemplateConfigs": [  
    {  
      "LaunchTemplateSpecification": {  
        "LaunchTemplateName": "my-launch-template",  
        "Version": "1"  
      },  
    },  
  ],  
}
```

```

    "Overrides": [
      {
        "InstanceType": "r4.2xlarge",
        "Priority": 1,
        "AvailabilityZone": "us-west-2a"
      },
      {
        "InstanceType": "m4.2xlarge",
        "Priority": 2,
        "AvailabilityZone": "us-west-2b"
      },
      {
        "InstanceType": "c5.2xlarge",
        "Priority": 3,
        "AvailabilityZone": "us-west-2b"
      }
    ]
  }
]
}

```

Exemple 11 : Lancer des instances ponctuelles dans une priceCapacityOptimized flotte

L'exemple suivant montre comment configurer un parc d'instances Spot avec une stratégie d'allocation Spot qui optimise la capacité et le prix le plus bas. Pour optimiser la capacité tout en tenant compte du prix, vous devez définir le Spot AllocationStrategy sur priceCapacityOptimized.

Dans l'exemple suivant, les trois spécifications de lancement spécifient trois groupes de capacités Spot. La capacité cible est de 50 instances Spot. Le parc d'instances Spot tente de lancer 50 instances Spot dans le groupe de capacités Spot avec une capacité optimale pour le nombre d'instances qui sont lancées, tout en choisissant également le groupe le moins cher.

```

{
  "SpotFleetRequestConfig": {
    "AllocationStrategy": "priceCapacityOptimized",
    "OnDemandAllocationStrategy": "lowestPrice",
    "ExcessCapacityTerminationPolicy": "default",
    "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
    "LaunchTemplateConfigs": [
      {

```

```
    "LaunchTemplateSpecification": {
      "LaunchTemplateId": "lt-0123456789example",
      "Version": "1"
    },
    "Overrides": [
      {
        "InstanceType": "r4.2xlarge",
        "AvailabilityZone": "us-west-2a"
      },
      {
        "InstanceType": "m4.2xlarge",
        "AvailabilityZone": "us-west-2b"
      },
      {
        "InstanceType": "c5.2xlarge",
        "AvailabilityZone": "us-west-2b"
      }
    ]
  },
  "TargetCapacity": 50,
  "Type": "request"
}
```

Exemple 12 : configurer la sélection de type d'instance basée sur des attributs

L'exemple suivant montre comment configurer un parc d'instances Spot pour qu'il utilise la sélection de type d'instance basée sur des attributs pour identifier les types d'instance. Pour spécifier les attributs d'instance requis, vous devez les spécifier dans la structure `InstanceRequirements`.

Dans l'exemple suivant, deux attributs d'instance sont spécifiés :

- `VCpuCount` : au moins 2 vCPU sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.
- `MemoryMiB` : au moins 4 Mio de mémoire sont spécifiés. Comme aucun maximum n'est spécifié, il n'y a pas de limite maximale.

Tout type d'instance doté d'au moins 2 vCPU et d'au moins 4 Mio de mémoire sera identifié.

Toutefois, la protection des prix et la stratégie d'allocation peuvent exclure certains types d'instances lorsque [le parc d'instances Spot alloue la flotte](#).

Pour obtenir une liste et une description de tous les attributs possibles que vous pouvez spécifier, consultez le [InstanceRequirements](#) manuel Amazon EC2 API Reference.

```
{
  "AllocationStrategy": "priceCapacityOptimized",
  "TargetCapacity": 20,
  "Type": "request",
  "LaunchTemplateConfigs": [{
    "LaunchTemplateSpecification": {
      "LaunchTemplateName": "my-launch-template",
      "Version": "1"
    }
  ],
  "Overrides": [{
    "InstanceRequirements": {
      "VCpuCount": {
        "Min": 2
      },
      "MemoryMiB": {
        "Min": 4
      }
    }
  ]
}]
}
```

Quotas liés aux flottes

Les quotas Amazon EC2 habituels (auparavant appelés limites) s'appliquent aux instances lancées par une flotte EC2 ou un parc d'instances Spot, tels que les [limites d'instance Spot](#) et les [limites de volume](#).

En outre, les quotas suivants s'appliquent :

Description du quota	Quota
Le nombre de flottes EC2 et de flottes ponctuelles par type de région maintin et request dans active les États deleted_running cancelled_running	1 000 ^{1 2 3}

Description du quota	Quota
Le nombre de flottes EC2 de type <code>instant</code>	Illimité
Le nombre de pools de capacité Spot (combinaison unique de type d'instance et de sous-réseau) pour les flottes EC2 et les flottes de type <code>maintain request</code>	300 ¹
Le nombre de pools de capacité Spot (combinaison unique de type d'instance et de sous-réseau) pour les flottes EC2 de type <code>instant</code>	Illimité
Taille des données utilisateur dans une spécification de lancement	16 Ko ²
Capacité cible par flotte EC2 ou parc d'instances Spot	10 000
Capacité cible pour tous les Flottes EC2 et Parcs d'instances Spot d'une région	100 000 ¹
Une demande de flotte EC2 ou une demande de parc d'instances Spot ne peut pas couvrir plusieurs régions.	
Une demande de flotte EC2 ou de parc d'instances Spot ne peut pas couvrir différents sous-réseaux de la même zone de disponibilité.	

¹ Ces quotas s'appliquent à vos Flottes EC2 et à vos Parcs d'instances Spot.

² Ces quotas sont finis. Vous ne pouvez pas demander une augmentation de ces quotas.

³ Après avoir supprimé une flotte EC2 ou annulé une demande de parc Spot, et si vous avez spécifié que la flotte ne doit pas mettre fin à ses instances ponctuelles lorsque vous avez supprimé ou annulé la demande, la demande de flotte entre dans l'état `deleted_running` (Flotte EC2) ou `cancelled_running` (Flotte d'instances Spot) et les instances continuent à être exécutées jusqu'à ce qu'elles soient interrompues ou jusqu'à ce que vous les mettiez hors service

manuellement. Si vous résiliez les instances, la demande de parc d'instances entre dans l'état `deleted_terminating` (Flotte EC2) ou `cancelled_terminating` (parc d'instances Spot) et ne compte pas dans ce quota. Pour plus d'informations, consultez [Supprimer une flotte EC2](#) et [Annulation d'une demande de parc d'instances Spot](#).

Demander une augmentation de quota pour la capacité cible

S'il vous faut un quota par défaut supérieur à la capacité cible, demandez une augmentation de quota.

Demander une augmentation de quota pour la capacité cible

1. Ouvrez le formulaire AWS Support Center [Create Case](#).
2. Sélectionnez Service Limit increase (Augmentation des limites de service).
3. Pour Limit type (Type de limite), choisissez EC2 Fleet (Flotte EC2).
4. Pour Région, choisissez la AWS région dans laquelle vous souhaitez demander l'augmentation du quota.
5. Pour Limit (Limite), choisissez Target Fleet Capacity per Fleet (in units) (Capacité cible de la flotte par flotte [en unités]) ou Target Fleet Capacity per Region (in units) (Capacité de flotte cible par région [en unités]), selon le quota que vous souhaitez augmenter.
6. Pour New limit value (Nouvelle valeur de la limite), saisissez la nouvelle valeur.
7. Pour demander l'augmentation d'un autre quota, choisissez Add another request (Ajouter une demande supplémentaire), et répétez les étapes 4 à 6.
8. Pour Use case description (Description du cas d'utilisation), indiquez la raison pour laquelle vous demandez une augmentation de quota.
9. Sous Contact options (Options de contact), spécifiez la langue de contact et la méthode de contact que vous préférez.
10. Sélectionnez Envoyer.

Surveiller Amazon EC2

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de vos instances Amazon Elastic Compute Cloud (Amazon EC2) et de vos solutions. AWS Vous devez collecter des données de surveillance provenant de tous les composants de vos AWS solutions afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. Cependant, avant de commencer à superviser Amazon EC2, créez un plan de surveillance qui inclut les questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

Une fois que vous avez défini vos objectifs de surveillance et créé votre plan de surveillance, l'étape suivante consiste à définir une référence pour les performances normales d'Amazon EC2 dans votre environnement. Vous devez mesurer les performances d'Amazon EC2 à différents moments et sous différentes conditions de charge. Lorsque vous surveillez Amazon EC2, stockez l'historique des données de surveillance que vous collectez. Vous pouvez comparer les performances actuelles d'Amazon EC2 à leurs données historiques pour vous aider à identifier les modèles de performances normales et les anomalies de performances, et à concevoir les méthodes destinées à les prendre en compte. Par exemple, vous pouvez superviser l'utilisation de l'UC, les I/O de disque et l'utilisation réseau de vos instances EC2. Lorsque les performances se trouvent en dehors de votre référence établie, il se peut que vous ayez besoin de reconfigurer l'instance ou de l'optimiser pour réduire l'utilisation de l'UC, améliorer les I/O disque ou réduire le trafic réseau.

Pour établir une référence, vous devez, au moins, superviser les éléments suivants :

Élément à superviser	Métrique Amazon EC2	Agent de surveillance/journaux CloudWatch
Utilisation de l'UC	CPUUtilization	

Élément à superviser	Métrique Amazon EC2	Agent de surveillance/journaux CloudWatch
Utilisation réseau	NetworkIn NetworkOut	
Performances disque	DiskReadOps DiskWriteOps	
Lectures/écritures sur disque	DiskReadOctets DiskWriteOctets	
Utilisation de la mémoire, des échanges, de l'espace sur le disque et du fichier d'échange, collecte de journaux		<p>[Instances de serveur Linux et Windows] Collectez des métriques et des journaux à partir d'instances Amazon EC2 et de serveurs sur site avec l'agent CloudWatch</p> <p>[Migration depuis l'ancien agent CloudWatch Logs sur les instances Windows Server] Migrer la collecte des journaux des instances Windows Server vers l' CloudWatch agent</p>

Surveillance automatique et surveillance manuelle

AWS fournit différents outils que vous pouvez utiliser pour surveiller Amazon EC2. Vous pouvez configurer certains outils pour qu'ils effectuent la supervision automatiquement, tandis que d'autres nécessitent une intervention manuelle.

Outils de surveillance

- [Outils de surveillance automatique](#)
- [Outils de surveillance manuelle](#)

Outils de surveillance automatique

Vous pouvez utiliser les outils de surveillance automatique pour surveiller Amazon EC2 et être informé en cas de problème :

- Contrôles de l'état du système : surveillez les AWS systèmes requis pour utiliser votre instance afin de vous assurer qu'ils fonctionnent correctement. Ces vérifications détectent les problèmes liés à votre instance qui nécessitent une AWS intervention pour les réparer. Lorsqu'un contrôle de statut échoue, vous pouvez choisir d'attendre qu' AWS résolve le problème ou le résoudre vous-même (par exemple, en arrêtant et en redémarrant une instance, ou en y mettant fin et en la remplaçant). Voici quelques exemples de problèmes entraînant l'échec des contrôles de statut du système :
 - Perte de connectivité réseau
 - Perte d'alimentation système
 - Problèmes logiciels sur un hôte physique
 - Problèmes matériels sur un hôte physique ayant un impact sur l'accessibilité du réseau

Pour plus d'informations, veuillez consulter [Contrôles de statut pour vos instances](#).

- Contrôles du statut de l'instance – Surveillez la configuration logicielle et réseau de votre instance. Ces contrôles détectent les problèmes nécessitant votre intervention pour les résoudre. Lorsqu'un contrôle du statut de l'instance échoue, vous devez généralement résoudre le problème vous-même (en redémarrant par exemple l'instance ou en apportant des modifications à votre système d'exploitation). Voici quelques exemples de problèmes susceptibles d'entraîner l'échec des contrôles du statut de l'instance :
 - Échec de contrôles de statut de système
 - Configuration de mise en réseau ou de démarrage incorrecte
 - Mémoire épuisée
 - Système de fichiers corrompu
 - Noyau incompatible

Pour plus d'informations, consultez [Contrôles de statut pour vos instances](#).

- CloudWatch Alarmes Amazon : surveillez une seule métrique sur une période que vous spécifiez et effectuez une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon Simple Notification Service (Amazon SNS) ou une politique Amazon EC2 Auto Scaling. Les alarmes déclenchent des actions uniquement pour les changements d'état prolongés.

CloudWatch les alarmes ne déclencheront pas d'actions simplement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Pour plus d'informations, consultez [Surveillez vos instances à l'aide de CloudWatch](#).

- Amazon EventBridge — automatisez vos AWS services et répondez automatiquement aux événements du système. Les événements issus AWS des services sont transmis EventBridge en temps quasi réel, et vous pouvez spécifier des actions automatisées à effectuer lorsqu'un événement correspond à une règle que vous avez écrite. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon EventBridge ?](#) .
- Amazon CloudWatch Logs : surveillez, stockez et accédez à vos fichiers journaux à partir d'instances Amazon EC2 ou d'autres sources. AWS CloudTrail Pour plus d'informations, consultez le [guide de l'utilisateur d'Amazon CloudWatch Logs](#).
- CloudWatch agent : collectez les journaux et les mesures au niveau du système auprès des hôtes et des invités sur vos instances EC2 et vos serveurs sur site. Pour plus d'informations, consultez la section [Collecte de métriques et de journaux à partir d'instances Amazon EC2 et de serveurs sur site avec l' CloudWatch agent dans le guide](#) de l'utilisateur Amazon CloudWatch .

Outils de surveillance manuelle

Un autre aspect important de la surveillance d'Amazon EC2 consiste à surveiller manuellement les éléments que les scripts de surveillance, les vérifications de statut et les CloudWatch alarmes ne couvrent pas. Les tableaux de bord Amazon EC2 et de CloudWatch la console fournissent un at-a-glance aperçu de l'état de votre environnement Amazon EC2.

- Le tableau de bord Amazon EC2 affiche :
 - État du service et événements planifiés par région
 - État de l'instance
 - Contrôles des statuts
 - Statut des alarmes
 - Détails des métriques d'instance (Dans le panneau de navigation, choisissez instances, sélectionnez une instance, et choisissez l'onglet Surveillance)
 - Détails des métriques de volume (Dans le panneau de navigation, choisissez Volumes, sélectionnez un volume, et choisissez l'onglet Surveillance)
- Le CloudWatch tableau de bord Amazon affiche :
 - Alarmes et statuts en cours

- Graphiques des alarmes et des ressources
- Statut d'intégrité du service

En outre, vous pouvez utiliser CloudWatch pour effectuer les opérations suivantes :

- Représenter graphiquement les données de surveillance Amazon EC2 pour résoudre les problèmes et découvrir les tendances
- Recherchez et parcourez tous les indicateurs de vos AWS ressources
- Créer et modifier des alarmes pour être informé des problèmes
- Consultez un at-a-glance aperçu de vos alarmes et AWS de vos ressources

Bonnes pratiques de surveillance

Utilisez les bonnes pratiques suivantes pour vous aider dans les tâches de surveillance d'Amazon EC2.

- Faites de la surveillance une priorité pour résoudre les petits problèmes avant qu'ils n'empirent.
- Créez et mettez en œuvre un plan de surveillance qui collecte les données de surveillance de tous les composants de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint le cas échéant. Votre plan de surveillance doit, au moins, traiter les questions suivantes :
 - Quels sont les objectifs de la surveillance ?
 - Quelles sont les ressources à surveiller ?
 - À quelle fréquence les ressources doivent-elles être surveillées ?
 - Quels outils de surveillance utiliser ?
 - Qui exécute les tâches de supervision ?
 - Qui doit être informé en cas de problème ?
- Automatisez les tâches de surveillance autant que possible.
- Vérifiez les fichiers journaux de vos instances EC2.

Surveiller le statut de vos instances

Vous pouvez surveiller le statut de vos instances en affichant les contrôles de statut et les événements planifiés pour vos instances.

Un contrôle de statut vous fournit les informations provenant de contrôles automatisés exécutés par Amazon EC2. Ces contrôles automatisés détectent si des problèmes spécifiques concernent vos instances. Les informations de vérification du statut, associées aux données fournies par Amazon CloudWatch, vous offrent une visibilité opérationnelle détaillée sur chacune de vos instances.

Vous pouvez également consulter le statut d'événements spécifiques planifiés pour vos instances. Les statuts des événements fournissent des informations sur les activités à venir planifiées pour vos instances, comme le redémarrage ou la mise hors service. Ils fournissent aussi les heures prévues de début et de fin de chaque événement.

Sommaire

- [Contrôles de statut pour vos instances](#)
- [Événements de changement d'état pour vos instances](#)
- [Événements planifiés pour vos instances.](#)

Contrôles de statut pour vos instances

Avec la surveillance du statut des instances, vous pouvez rapidement déterminer si Amazon EC2 a détecté des problèmes susceptibles d'empêcher vos instances d'exécuter des applications. Amazon EC2 exécute des contrôles automatisés sur chaque instance EC2 en cours d'exécution pour identifier les problèmes matériels et logiciels. Vous pouvez afficher les résultats de ces contrôles de statut pour identifier des problèmes spécifiques et détectables. Les données d'état des événements complètent les informations déjà fournies par Amazon EC2 concernant l'état de chaque instance (par exemple `running`, `stopping`,) et les mesures d'utilisation surveillées par CloudWatch Amazon (utilisation du processeur, trafic réseau et activité du disque). `pending`

Les contrôles de statut sont exécutés toutes les minutes et chacun d'entre eux renvoie un statut de réussite ou d'échec. Si tous les contrôles réussissent, le statut global de l'instance est OK. Si un ou plusieurs contrôles échouent, le statut global de l'instance est dégradé. Les contrôles de statut sont intégrés à Amazon EC2. Ils ne peuvent donc pas être désactivés ou supprimés.

Lorsqu'une vérification de statut échoue, la CloudWatch métrique correspondante pour les vérifications de statut est incrémentée. Pour plus d'informations, consultez [Métriques de contrôle de statut](#). Vous pouvez utiliser ces mesures pour créer des CloudWatch alarmes déclenchées en fonction du résultat des vérifications d'état. Par exemple, vous pouvez créer une alarme pour vous avertir si des contrôles de statut échouent sur une instance spécifique. Pour plus d'informations, consultez [Créer et modifier des alarmes de vérification de statut](#).

Vous pouvez également créer une CloudWatch alarme Amazon qui surveille une instance Amazon EC2 et la récupère automatiquement si elle est altérée en raison d'un problème sous-jacent. Pour plus d'informations, consultez [Résilience de l'instance](#).

Sommaire

- [Types de contrôles de statut](#)
- [Travailler avec les contrôles de statut](#)

Types de contrôles de statut

Il existe trois types de contrôles de statuts.

- [Contrôles de statut de système](#)
- [Contrôles de statut des instances](#)
- [Contrôles de statut de l'EBS attaché](#)

Contrôles de statut de système

Les vérifications de l'état du système surveillent les AWS systèmes sur lesquels votre instance s'exécute. Ces contrôles détectent les problèmes sous-jacents liés à votre instance qui nécessitent une intervention de résolution d' AWS . Lorsqu'une vérification de l'état du système échoue, vous pouvez choisir AWS d'attendre que le problème soit résolu ou de le résoudre vous-même. Pour les instances basées sur Amazon EBS, vous pouvez arrêter et démarrer l'instance vous-même, ce qui, dans la plupart des cas, entraîne la migration de l'instance vers un nouvel hôte. Pour les instances Linux basées sur le stockage d'instance, vous pouvez mettre l'instance hors service et la remplacer. Pour les instances Windows, le volume racine doit être un volume Amazon EBS ; le stockage d'instance n'est pas pris en charge pour le volume racine. Notez que les volumes de stockage d'instance sont éphémères et que toutes les données sont perdues lorsque l'instance est arrêtée.

Voici des exemples de problèmes pouvant entraîner l'échec des contrôles de statut :

- Perte de connectivité réseau
- Perte d'alimentation système
- Problèmes logiciels sur un hôte physique
- Problèmes matériels sur un hôte physique ayant un impact sur l'accessibilité du réseau

Si la vérification de l'état du système échoue, nous incrémentons la métrique [StatusCheckFailed_System](#).

Instances nues

Si vous effectuez un redémarrage à partir du système d'exploitation sur une instance nue (bare metal), la vérification de l'état du système peut renvoyer temporairement un état d'échec. Lorsque l'instance devient disponible, la vérification de l'état du système doit renvoyer un état de succès.

Contrôles de statut des instances

Contrôles du statut de l'instance Surveillez la configuration logicielle et réseau de votre instance. Amazon EC2 vérifie l'état de l'instance en envoyant une demande de protocole de résolution d'adresse (ARP) à l'interface réseau (NIC). Ces contrôles détectent les problèmes nécessitant votre intervention pour les résoudre. Lorsqu'un contrôle de statut d'instance échoue, vous devez généralement résoudre le problème vous-même (par exemple, en redémarrant l'instance ou en effectuant des changements de configuration sur l'instance).

Note

Les distributions Linux récentes utilisées `systemd-networkd` pour la configuration réseau peuvent rendre compte des vérifications de santé différemment des distributions précédentes. Au cours du processus de démarrage, ce type de réseau peut démarrer plus tôt et éventuellement se terminer avant d'autres tâches de démarrage susceptibles d'affecter l'état de l'instance. Les vérifications d'état qui dépendent de la disponibilité du réseau peuvent signaler un état sain avant la fin des autres tâches.

Voici des exemples de problèmes pouvant entraîner l'échec des contrôles d'instance :

- Échec de contrôles de statut de système
- Configuration de mise en réseau ou de démarrage incorrecte
- Mémoire épuisée
- Système de fichiers corrompu
- Noyau incompatible
- [Instances Windows] Lors du redémarrage de l'instance ou lorsqu'une instance basée sur le stockage d'une instance Windows est groupée, une vérification de l'état de l'instance signale un échec jusqu'à ce que l'instance soit de nouveau disponible.

Si la vérification de l'état d'une instance échoue, nous incrémentons la métrique [StatusCheckFailed_Instance](#).

Instances nues

Si vous effectuez un redémarrage à partir du système d'exploitation sur une instance nue (bare metal), la vérification de l'état de l'instance peut renvoyer temporairement un état d'échec. Lorsque l'instance devient disponible, la vérification de l'état de l'instance doit renvoyer un état de succès.

Contrôles de statut de l'EBS attaché

Les contrôles de statut de l'EBS attaché vérifient si les volumes Amazon EBS attachés à une instance sont accessibles et capables d'effectuer des opérations d'E/S. La métrique `StatusCheckFailed_AttachedEBS` est une valeur binaire qui indique une altération si un ou plusieurs volumes EBS attachés à l'instance ne sont pas en mesure d'effectuer les opérations d'E/S. Ces vérifications de statut détectent les problèmes sous-jacents liés au calcul ou à l'infrastructure Amazon EBS. Lorsque la métrique de vérification du statut EBS jointe échoue, vous pouvez soit attendre AWS que le problème soit résolu, soit prendre des mesures, telles que le remplacement des volumes concernés ou l'arrêt et le redémarrage de l'instance.

Vous trouverez ci-dessous des exemples de problèmes pouvant entraîner l'échec des contrôles de statut de l'EBS attaché :

- Problèmes matériels ou logiciels sur les sous-systèmes de stockage sous-jacents aux volumes EBS
- Problèmes matériels sur l'hôte physique ayant un impact sur l'accessibilité des volumes EBS
- Problèmes de connectivité entre l'instance et les volumes EBS

Vous pouvez utiliser la métrique `StatusCheckFailed_AttachedEBS` pour améliorer la résilience de votre charge de travail. Vous pouvez utiliser cette métrique pour créer des CloudWatch alarmes Amazon déclenchées en fonction du résultat de la vérification de statut. Par exemple, vous pouvez basculer vers une instance secondaire ou une zone de disponibilité lorsque vous détectez un impact prolongé. Vous pouvez également surveiller les performances d'E/S de chaque volume connecté à l'aide des CloudWatch métriques EBS pour détecter et remplacer le volume endommagé. Si votre charge de travail ne génère aucune E/S vers des volumes EBS attachés à votre instance et que le contrôle de statut de l'EBS attaché indique un dysfonctionnement, vous pouvez arrêter et redémarrer l'instance pour résoudre les problèmes liés à l'hôte physique qui ont un impact sur l'accessibilité des

volumes EBS. Pour plus d'informations, consultez les [CloudWatch métriques Amazon pour Amazon EBS](#)

Note

- La métrique de contrôle de statut de l'EBS attaché n'est disponible que pour les instances Nitro.
- Vous pouvez surveiller la métrique de vérification de statut EBS jointe en [créant une CloudWatch alarme](#) basée sur la `StatusCheckFailed_AttachedEBS` métrique. Vous ne pouvez pas afficher cette vérification d'état à l'aide de la commande [AWS CLI describe-instance-status](#).

Travailler avec les contrôles de statut

Vous pouvez effectuer des contrôles de statut à l'aide de la console et des outils de ligne de commande, tels que AWS CLI.

Rubriques

- [Afficher les vérifications de statut](#)
- [Créer et modifier des alarmes de vérification de statut](#)

Afficher les vérifications de statut

Pour consulter les contrôles de statut, utilisez l'une des méthodes suivantes.

Console

Pour afficher les contrôles de statut

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez instances.
3. Sur la page instances, la colonne Status check (Vérification de statut) répertorie le statut opérationnel de chaque instance.
4. Pour afficher le statut d'une instance spécifique, sélectionnez-la, puis choisissez l'onglet Statuts et alarmes.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availi
spot-instance-2	i-01aeed690c9fb5322	Running	t3.nano	1/2 checks ...	View alarms +	eu-w
spot-instance-1	i-0ba5e5bbc9d634fa6	Stopped	t3.nano	-	View alarms +	eu-w
EIC-RHEL	i-08e66e73da739c7f4	Running	t2.micro	2/2 checks passed	View alarms +	eu-w
Windows	i-0cb952751a0d8388b	Running	t3.nano	2/2 checks passed	View alarms +	eu-w

Instance: i-01aeed690c9fb5322 (spot-instance-2)

Details | **Status and alarms New** | Monitoring | Security | Networking | Storage | Tags

Status checks Info
 Status checks detect problems that may impair i-01aeed690c9fb5322 (spot-instance-2) from running your applications.

System status checks

- System reachability check passed

► Metrics

▼ Alarms

Instance status checks

- Instance reachability check failed
Check failure at 2020/12/16 17:30 GMT+2 (about 1 month)

Find alarms by name

Name	State	Description	Metric name	State reason
Instance has no associated alarms				

Lorsqu'un contrôle de statut d'instance échoue, vous devez généralement résoudre le problème vous-même (par exemple, en redémarrant l'instance ou en effectuant des changements de configuration sur celle-ci). Pour résoudre les problèmes liés aux échecs de vérification de l'état du système ou de l'instance sur les instances Linux, consultez [Résoudre les problèmes des instances Linux dont les vérifications d'état ont échoué](#).

- Pour consulter les CloudWatch mesures relatives aux vérifications de statut, dans l'onglet État et alarmes, développez Métriques pour afficher les graphiques des mesures suivantes :
 - Échec du contrôle de statut au niveau du système
 - Échec du contrôle de statut au niveau de l'instance

Pour plus d'informations, consultez [the section called "Métriques de contrôle de statut"](#).

Command line

Vous pouvez afficher des vérifications du statut des instances en cours d'exécution à l'aide de la commande [describe-instance-status](#) (AWS CLI).

Pour afficher le statut de toutes les instances, utilisez la commande suivante :

```
aws ec2 describe-instance-status
```

Pour obtenir le statut de toutes les instances avec un statut d'instance `impaired`, utilisez la commande suivante.

```
aws ec2 describe-instance-status \  
  --filters Name=instance-status.status,Values=impaired
```

Pour obtenir le statut d'une seule instance, utilisez la commande suivante.

```
aws ec2 describe-instance-status \  
  --instance-ids i-1234567890abcdef0
```

Vous pouvez également utiliser les commandes suivantes :

- [Get-EC2InstanceStatus](#) (AWS Tools for Windows PowerShell)
- [DescribeInstanceÉtat](#) (API de requête Amazon EC2)

Si la vérification de l'état d'une instance Linux a échoué, consultez [Résoudre les problèmes des instances Linux dont les vérifications d'état ont échoué](#).

Créer et modifier des alarmes de vérification de statut

Vous pouvez utiliser les [métriques de vérification de statut](#) pour créer des CloudWatch alarmes afin de vous avertir en cas d'échec de la vérification de statut d'une instance.

Important

Les contrôles d'état et les alarmes de contrôle d'état peuvent temporairement passer à un état de données insuffisant s'il manque des points de données métriques. Bien que cela soit rare, cela peut se produire en cas d'interruption des systèmes de reporting des métriques, même lorsqu'une instance est saine. Nous vous recommandons de traiter cet état comme une donnée manquante plutôt que comme un échec de vérification du statut ou comme une violation d'alarme, en particulier lorsque vous effectuez des actions d'arrêt, de terminaison, de redémarrage ou de restauration sur l'instance en réponse.

Pour créer une alarme de contrôle de statut, utilisez l'une des méthodes suivantes :

Console

Utilisez la procédure suivante pour configurer une alarme qui vous envoie une notification par e-mail, ou arrête, met fin ou récupère une instance en cas d'échec du contrôle de statut de cette dernière.

Pour créer une alarme de contrôle de statut

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez instances.
3. Sélectionnez l'instance, choisissez l'onglet Status Checks (Contrôles des statuts), puis choisissez Actions, Create status check alarm (Créer une alarme de contrôle de statut).
4. Sur la page Gérer les CloudWatch alarmes, sous Ajouter ou modifier une alarme, choisissez Créer une alarme.
5. Pour Alarm notification (Notification d'alarme), activez ou désactivez les notifications Amazon Simple Notification Service (Amazon SNS). Sélectionnez une rubrique Amazon SNS existante ou entrez un nom pour créer une nouvelle rubrique.

Si vous avez ajouté une adresse e-mail à la liste de destinataires ou créé une nouvelle rubrique, Amazon SNS envoie un e-mail de confirmation d'abonnement à chaque nouvelle adresse. Chaque destinataire doit confirmer l'abonnement en choisissant le lien contenu dans ce message. Les notifications d'alerte sont envoyées uniquement aux adresses confirmées.

6. Activez Alarm action (Action d'alarme) pour spécifier une action à effectuer lorsque l'alarme est déclenchée. Sélectionnez l'action.
7. Pour Alarm thresholds (Seuils d'alarme), sélectionnez la métrique et les critères de l'alarme.

Vous pouvez laisser les paramètres par défaut pour Regrouper les échantillons par (moyenne) et Type de données à échantillonner (échec de la vérification de statut : soit), ou vous pouvez les modifier en fonction de vos besoins.

Dans Consecutive period (Période consécutive), définissez le nombre de périodes que vous souhaitez évaluer et, dans Period (Période), sélectionnez la période d'évaluation avant de déclencher l'alarme et d'envoyer un e-mail.

8. (Facultatif) Pour Exemple de données de métrique, choisissez Ajouter au tableau de bord.
9. Sélectionnez Créer.

Si vous devez apporter des modifications à une alarme de statut d'instance, vous pouvez modifier celle-ci.

Pour modifier une alarme de contrôle de statut

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveillance, Gestion des CloudWatch alarmes.
4. Sur la page Gérer les CloudWatch alarmes, sous Ajouter ou modifier une alarme, choisissez Modifier une alarme.
5. Dans Search for alarm (Rechercher une alarme), sélectionnez l'alarme.
6. Une fois les modifications terminées, sélectionnez Update (Mettre à jour).

Command line

Dans l'exemple suivant, l'alarme publie une notification dans une rubrique SNS, `arn:aws:sns:us-west-2:111122223333:my-sns-topic`, lorsque l'instance échoue lors d'un contrôle de statut d'instance ou un contrôle de statut de système pour au moins deux périodes consécutives. La CloudWatch métrique utilisée est `StatusCheckFailed`.

Pour créer une alarme de vérification de statut à l'aide du AWS CLI

1. Sélectionnez une rubrique SNS existante ou créez-en une nouvelle. Pour plus d'informations, consultez la section [Utilisation du service AWS CLI avec Amazon SNS](#) dans le guide de l'AWS Command Line Interface utilisateur.
2. Utilisez la commande [list-metrics](#) suivante pour afficher les métriques Amazon disponibles pour Amazon CloudWatch EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Utilisez la commande [put-metric-alarm](#) suivante pour créer l'alarme.

```
aws cloudwatch put-metric-alarm \  
  --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \  
  --metric-name StatusCheckFailed \  
  --namespace AWS/EC2 \  
  --statistic Maximum \  
  --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \  
  --
```

```
--unit Count \  
--period 300 \  
--evaluation-periods 2 \  
--threshold 1 \  
--comparison-operator GreaterThanOrEqualToThreshold \  
--alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

La période est la période, en secondes, pendant laquelle CloudWatch les métriques Amazon sont collectées. Dans cet exemple, 300, qui correspond à 60 secondes multipliées par 5 minutes, est utilisé. La période d'évaluation est le nombre de périodes consécutives pour lesquelles la valeur de la métrique doit être comparée au seuil. Dans cet exemple, 2 est utilisé. Les actions d'alarme correspondent aux actions à exécuter lors du déclenchement de cette alarme. Dans cet exemple, l'alarme est configurée pour envoyer un e-mail à l'aide de Amazon SNS.

Événements de changement d'état pour vos instances

Amazon EC2 envoie un EC2 Instance State-change Notification événement à Amazon EventBridge lorsque l'état d'une instance change.

Voici un exemple de données pour cet événement. Dans cet exemple, l'instance est entrée dans l'état pending.

```
{  
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",  
  "detail-type": "EC2 Instance State-change Notification",  
  "source": "aws.ec2",  
  "account": "123456789012",  
  "time": "2021-11-11T21:29:54Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"  
  ],  
  "detail": {  
    "instance-id": "i-abcd1111",  
    "state": "pending"  
  }  
}
```

Les valeurs possibles pour state sont :

- pending
- running
- stopping
- stopped
- shutting-down
- terminated

Lorsque vous lancez ou démarrez une instance, elle entre dans l'état `pending`, puis dans l'état `running`. Lorsque vous arrêtez une instance, elle entre dans l'état `stopping`, puis dans l'état `stopped`. Lorsque vous résiliez une instance, elle entre dans l'état `shutting-down`, puis dans l'état `terminated`.

Recevoir une notification par e-mail lorsqu'une instance change d'état

Pour recevoir des notifications par e-mail lorsque votre instance change d'état, créez une rubrique Amazon SNS, puis créez une EventBridge règle pour l'EC2 Instance State-change Notification événement.

Pour créer une rubrique SNS

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans le volet de navigation, choisissez Rubriques.
3. Choisissez Créer une rubrique.
4. Pour Type, choisissez Standard.
5. Pour Nom, saisissez un nom pour votre rubrique.
6. Choisissez Créer une rubrique.
7. Choisissez Créer un abonnement.
8. Pour Protocole, choisissez E-mail.
9. Pour Point de terminaison, saisissez l'adresse e-mail qui reçoit les notifications.
10. Choisissez Créer un abonnement.
11. Vous recevrez un e-mail avec l'objet suivant : AWS Notification - Subscription Confirmation. Suivez les instructions pour confirmer votre abonnement.

Pour créer une EventBridge règle

1. Ouvrez la EventBridge console Amazon à l'[adresse https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Choisissez Créer une règle.
3. Pour Nom, saisissez un nom pour votre règle.
4. Pour Type de règle, choisissez Règle avec un modèle d'événement.
5. Choisissez Suivant.
6. Pour Event pattern (Modèle d'événement), procédez comme suit :
 - a. Pour Event source (Source d'événement), choisissez Services AWS.
 - b. Pour Service AWS, choisissez EC2.
 - c. Pour Event Type (Type d'événement), sélectionnez EC2 Instance State-change Notification (Notification de changement d'état de l'instance EC2).
 - d. Par défaut, nous envoyons des notifications pour tout changement d'état pour n'importe quelle instance. Si vous préférez, vous pouvez sélectionner des états ou des instances spécifiques.
7. Choisissez Suivant.
8. Spécifiez une cible comme suit :
 - a. Pour Target types (Types de cibles), choisissez Service AWS.
 - b. Pour Select a target (Sélectionnez une cible), choisissez SNS Topic (Rubrique SNS).
 - c. Pour Topic (Rubrique), choisissez la rubrique SNS que vous avez créée au cours de la procédure précédente.
9. Choisissez Suivant.
10. (Facultatif) Ajoutez des identifications à votre règle.
11. Choisissez Suivant.
12. Choisissez Créer une règle.
13. Pour tester votre règle, déclenchez un changement d'état. Par exemple, démarrez une instance arrêtée, arrêtez une instance en cours d'exécution ou lancez une instance. Vous recevrez des e-mails avec l'objet suivant : AWS Notification Message. Le corps de l'e-mail contient les données de l'événement.

Événements planifiés pour vos instances.

AWS peut planifier des événements pour vos instances, tels qu'un redémarrage, un arrêt/démarrage ou une mise hors service. Ces événements ne se produisent pas fréquemment. Si l'une de vos instances est affectée par un événement programmé, AWS envoie un e-mail à l'adresse e-mail associée à votre AWS compte avant l'événement prévu. Cet e-mail fournit des détails concernant l'événement, y compris les dates de début et de fin. En fonction de l'événement, vous pouvez peut-être prendre des mesures pour contrôler le calendrier de l'événement. AWS envoie également un AWS Health événement, que vous pouvez surveiller et gérer à l'aide d'Amazon CloudWatch Events. Pour plus d'informations sur la surveillance des AWS Health événements avec CloudWatch, consultez la section [Surveillance AWS Health des événements avec CloudWatch des événements](#).

Les événements planifiés sont gérés par AWS ; vous ne pouvez pas planifier d'événements pour vos instances. Vous pouvez consulter les événements planifiés par AWS, personnaliser les notifications d'événements planifiés pour inclure ou supprimer des balises dans la notification par e-mail, et effectuer des actions lorsqu'il est prévu de redémarrer, de retirer ou d'arrêter une instance.

Pour mettre à jour les informations de contact de votre compte afin d'être sûr d'être averti à propos d'événements planifiés, accédez à la page [Account Settings \(Paramètres du compte\)](#).

Note

Lorsqu'une instance est affectée par un événement planifié et qu'elle fait partie d'un groupe Auto Scaling, Amazon EC2 Auto Scaling finit par la remplacer dans le cadre de ses surveillances de l'état, sans aucune autre action nécessaire de votre part. Pour plus d'informations sur les surveillances de l'état réalisées par Amazon EC2 Auto Scaling, consultez [Vérification de l'état des instances Auto Scaling](#) dans le Amazon EC2 Auto Scaling Guide de l'utilisateur.

Table des matières

- [Types d'événements planifiés](#)
- [Afficher les événements planifiés](#)
- [Personnaliser les notifications d'événements planifiés](#)
- [Gérer les instances planifiées pour être arrêtées ou retirées](#)
- [Gérer les instances planifiées pour un reboot](#)

- [Gérer les instances planifiées pour une maintenance](#)
- [Replanifier un événement planifié](#)
- [Définir des fenêtres d'événements pour des événements planifiés](#)

Types d'événements planifiés

Amazon EC2 peut créer les types d'événements suivants pour vos instances, où l'événement se produit à une heure planifiée :

- Instance stop (Arrêt de l'instance) : à l'heure planifiée, l'instance est arrêté. Lorsque vous la redémarrez, elle est migrée vers un nouvel hôte. S'applique uniquement aux instances basées sur Amazon EBS.
- Instance retirement (Mise hors service d'instance) : à l'heure planifiée, l'instance est arrêtée si elle est soutenue par Amazon EBS ou mise hors service si elle est soutenue par un stockage d'instance.
- Instance reboot (Redémarrage de l'instance) : à l'heure planifiée, l'instance est redémarrée.
- System reboot (Redémarrage du système) : à l'heure planifiée, l'hôte de l'instance est redémarré.
- System maintenance (Maintenance du système) : à l'heure planifiée, l'instance peut être temporairement affectée par une maintenance du réseau ou une maintenance de l'alimentation.

Afficher les événements planifiés

En plus de recevoir une notification des événements planifiés par e-mail, vous pouvez consulter les événements planifiés en utilisant une des méthodes suivantes.

Console

Pour afficher les événements planifiés pour vos instances

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Le tableau de bord affiche toutes les ressources avec un événement associé sous Événements planifiés.

Scheduled events ↻

US East (N. Virginia)

- 7 instance(s) have scheduled events
- 1 volume(s) are impaired

3. Pour obtenir plus de détails, sélectionnez Événements dans le volet de navigation. Toutes les ressources avec un événement associé sont affichées. Vous pouvez filtrer par caractéristiques telles que le type d'événement, le type de ressource et la zone de disponibilité.

Events (103) ↻ Actions ▾

< 1 > ⚙

Resource type: instance ✕
Event status: Scheduled ✕
Event type: instance-stop ✕
Clear filters

<input type="checkbox"/>	Resource ID	Event status	Event type	Description	Progress	Duration	Start time
<input type="checkbox"/>	i-02c48fffa61cd16f	🕒 Scheduled	instance-stop	The instance is running on ...	Starts in 13 days		2019/07/22 13:00 GMT+2

AWS CLI

Pour afficher les événements planifiés pour vos instances

Utilisez la commande [describe-instance-status](#).

```
aws ec2 describe-instance-status \
  --instance-id i-1234567890abcdef0 \
  --query "InstanceStatuses[.].Events"
```

L'exemple de sortie suivant montre un événement de redémarrage :

```
[
  "Events": [
    {
      "InstanceEventId": "instance-event-0d59937288b749b32",
      "Code": "system-reboot",
      "Description": "The instance is scheduled for a reboot",
```

```
        "NotAfter": "2019-03-15T22:00:00.000Z",
        "NotBefore": "2019-03-14T20:00:00.000Z",
        "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
    }
]
]
```

Voici un exemple de sortie montrant un événement de mise hors service d'instance.

```
[
  "Events": [
    {
      "InstanceEventId": "instance-event-0e439355b779n26",
      "Code": "instance-stop",
      "Description": "The instance is running on degraded hardware",
      "NotBefore": "2015-05-23T00:00:00.000Z"
    }
  ]
]
```

PowerShell

Pour afficher les événements planifiés pour vos instances à l'aide de la AWS Tools for Windows PowerShell

Utilisez la commande [Get-EC2InstanceStatus](#) suivante.

```
PS C:\> (Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

Voici un exemple de sortie montrant un événement de mise hors service d'instance.

```
Code           : instance-stop
Description    : The instance is running on degraded hardware
NotBefore      : 5/23/2015 12:00:00 AM
```

Instance metadata

Pour afficher les événements planifiés pour vos instances à l'aide des métadonnées de l'instance

Vous pouvez récupérer des informations sur les événements de maintenance actifs pour vos instances à partir des [métadonnées de l'instance](#) à l'aide de Service des métadonnées d'instance Version 2 ou Service des métadonnées d'instance Version 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

Voici un exemple de sortie avec des informations sur un événement de redémarrage système planifié, au format JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

Pour afficher l'historique des événements terminés ou annulés pour vos instances à l'aide des métadonnées de l'instance

Vous pouvez récupérer des informations sur les événements terminés ou annulés pour vos instances à partir des [métadonnées de l'instance](#) à l'aide de Service des métadonnées d'instance Version 2 ou Service des métadonnées d'instance Version 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

Voici un exemple de sortie avec des informations sur un événement de redémarrage du système qui a été annulé et un événement de redémarrage du système qui a été terminé, au format JSON.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

Vous pouvez utiliser le AWS Health Dashboard pour en savoir plus sur les événements susceptibles d'affecter votre instance. Il AWS Health Dashboard organise les problèmes en trois groupes : les problèmes ouverts, les modifications planifiées et les autres notifications. Le groupe des modifications planifiées contient des éléments qui sont en cours ou à venir.

Pour plus d'informations, consultez [Premiers pas avec le AWS Health Dashboard](#) dans le Guide de l'utilisateur AWS Health .

Personnaliser les notifications d'événements planifiés

Vous pouvez personnaliser les notifications d'événements planifiés pour inclure des balises dans la notification par e-mail. Cela facilite l'identification de la ressource affectée (instances ou Hôtes dédiés) et la hiérarchisation des actions pour l'événement à venir.

Lorsque vous personnalisez les notifications d'événements pour inclure des balises, vous pouvez choisir d'inclure :

- Toutes les balises associées à la ressource affectée
- Seules les balises spécifiques associées à la ressource affectée

Par exemple, supposons que vous assignez les balises `application`, `costcenter`, `project` et `owner` à toutes vos instances. Vous pouvez choisir d'inclure toutes les balises dans les notifications d'événements. Sinon, si vous souhaitez afficher uniquement les balises `owner` et `project` dans les notifications d'événements, vous pouvez choisir d'inclure uniquement ces balises.

Après avoir sélectionné les balises à inclure, les notifications d'événement incluront l'ID de ressource (ID d'instance ou Hôte dédié) et les paires clé de balise et valeur associées à la ressource affectée.

Tâches

- [Inclure des balises dans les notifications d'événements](#)
- [Supprimer les balises des notifications d'événements](#)
- [Afficher les balises à inclure dans les notifications d'événements](#)

Inclure des balises dans les notifications d'événements

Les balises que vous choisissez d'inclure s'appliquent à toutes les ressources (instances et Hôtes dédiés) de la région sélectionnée. Pour personnaliser les notifications d'événements dans d'autres régions, sélectionnez d'abord la région requise, puis effectuez les étapes suivantes.

Vous pouvez inclure des étiquettes dans les notifications d'événements à l'aide de l'une des méthodes suivantes.

Console

Pour inclure des balises dans les notifications d'événements

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Manage event notifications (Gérer les notifications d'événements).
4. Activez Inclure des balises dans les notifications d'événements.
5. Faites l'une des opérations suivantes, en fonction des balises que vous souhaitez inclure dans les notifications d'événement :
 - Pour inclure toutes les balises associées à l'instance affectée ou Hôte dédié, sélectionnez Inclure toutes les balises de ressource.
 - Pour sélectionner les balises à inclure, sélectionnez Choisir les balises à inclure, puis sélectionnez ou saisissez les clés de balise.
6. Choisissez Enregistrer.

AWS CLI

Pour inclure toutes les balises dans les notifications d'événements

Utilisez la commande [register-instance-event-notification-attributes](#) de l' AWS CLI et définissez le paramètre `IncludeAllTagsOfInstance` sur `true`.

```
aws ec2 register-instance-event-notification-attributes \  
  --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

Pour inclure des balises spécifiques dans les notifications d'événements

Utilisez la commande [register-instance-event-notification-attributes](#) de la AWS CLI et spécifiez les étiquettes à inclure avec le paramètre `InstanceTagKeys`.

```
aws ec2 register-instance-event-notification-attributes \  
  --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",  
  "tag_key_3"]'
```

Supprimer les balises des notifications d'événements

Vous pouvez supprimer les étiquettes des notifications d'événements à l'aide de l'une des méthodes suivantes.

Console

Pour supprimer les balises des notifications d'événements

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Manage event notifications (Gérer les notifications d'événements).
4. Pour supprimer toutes les balises des notifications d'événement, désactivez Inclure des balises dans les notifications d'événement.
5. Pour supprimer des balises spécifiques des notifications d'événements, sélectionnez le X) pour les clés de balise correspondantes.
6. Choisissez Enregistrer.

AWS CLI

Pour supprimer toutes les balises des notifications d'événements

Utilisez la commande [deregister-instance-event-notification-attributes](#) de l' AWS CLI et définissez le paramètre `IncludeAllTagsOfInstance` sur `false`.

```
aws ec2 deregister-instance-event-notification-attributes \  
  --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

Pour supprimer des balises spécifiques des notifications d'événements

Utilisez la AWS CLI commande [deregister-instance-event-notification-attributes](#) et spécifiez les balises à supprimer à l'aide du `InstanceTagKeys` paramètre.

```
aws ec2 deregister-instance-event-notification-attributes \  
  --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",  
  "tag_key_3"]'
```

Afficher les balises à inclure dans les notifications d'événements

Vous pouvez afficher les étiquettes qui doivent être incluses dans les notifications d'événement à l'aide de l'une des méthodes suivantes.

Console

Pour afficher les balises à inclure dans les notifications d'événements

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Manage event notifications (Gérer les notifications d'événements).

AWS CLI

Pour afficher les balises à inclure dans les notifications d'événements

Utilisez la commande [describe-instance-event-notification AWS CLI -attributes](#).

```
aws ec2 describe-instance-event-notification-attributes
```

Gérer les instances planifiées pour être arrêtées ou retirées

Lorsqu'il AWS détecte une défaillance irréparable de l'hôte sous-jacent de votre instance, il planifie l'arrêt ou la résiliation de l'instance, en fonction du type de périphérique racine de l'instance. Si le périphérique racine est un volume EBS, l'arrêt de l'instance est planifié. Si le périphérique racine est un volume de stockage d'instance, la fin de l'instance est planifiée. Pour plus d'informations, veuillez consulter [Mise hors service d'instance](#).

Important

Les données stockées sur des volumes de stockage d'instance sont perdues lorsque l'instance est arrêtée, mise en veille prolongée ou résiliée. Ceci inclut les volumes de stockage d'instance attachés à une instance ayant un volume EBS comme périphérique racine. Veillez à enregistrer les données de vos volumes de stockage d'instance dont vous aurez besoin ultérieurement avant que l'instance ne soit arrêtée, mise en veille prolongée ou résiliée.

Actions pour les instances basées sur Amazon EBS

Vous pouvez attendre que l'instance s'arrête comme planifié. Sinon, vous pouvez arrêter et démarrer l'instance vous-même, ce qui la migre vers un nouvel ordinateur hôte. Pour plus d'informations sur

l'arrêt de votre instance, ainsi que des informations sur les changements apportés à la configuration de votre instance lorsque celle-ci est arrêtée, consultez [Arrêtez et démarrez les instances Amazon EC2](#).

Vous pouvez automatiser un arrêt immédiat et un démarrage en réponse à un événement planifié d'arrêt d'instance. Pour plus d'informations, veuillez consulter la rubrique [Automating actions for Amazon EC2 instances](#) dans le Guide de l'utilisateur AWS Health .

Actions pour les instances basées sur le stockage d'instance

Nous vous recommandons de lancer une instance de remplacement à partir de votre AMI la plus récente et de migrer toutes les données nécessaires vers l'instance de remplacement avant que l'instance ne soit planifiée pour prendre fin. Ensuite, vous pouvez mettre fin à l'instance d'origine ou attendre que l'instance prenne fin comme planifié.

Gérer les instances planifiées pour un reboot

Lorsqu' AWS il doit effectuer des tâches telles que l'installation de mises à jour ou la maintenance de l'hôte sous-jacent, il peut planifier le redémarrage de l'instance ou de l'hôte sous-jacent. Vous pouvez [reprogrammer la plupart des événements de redémarrage](#) afin que votre instance soit redémarrée à une date et une heure spécifiques qui vous conviennent.

Afficher le type d'événement de reboot

Vous pouvez déterminer si l'événement de redémarrage est un redémarrage d'instance ou de système à l'aide de l'une des méthodes suivantes.

Console

Pour afficher le type d'événement de redémarrage planifié

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Type de ressource : instance dans la liste des filtres.
4. Pour chaque instance, affichez la valeur dans la colonne Type d'événement. La valeur est soit system-reboot (redémarrage du système), soit instance-reboot (redémarrage de l'instance).

AWS CLI

Pour afficher le type d'événement de redémarrage planifié

Utilisez la commande [describe-instance-status](#).

```
aws ec2 describe-instance-status \  
  --instance-id i-1234567890abcdef0
```

Pour les événements de redémarrage programmés, la valeur de Code est soit `system-reboot` ou `instance-reboot`. L'exemple de sortie suivant affiche un événement `system-reboot`.

```
[  
  "Events": [  
    {  
      "InstanceEventId": "instance-event-0d59937288b749b32",  
      "Code": "system-reboot",  
      "Description": "The instance is scheduled for a reboot",  
      "NotAfter": "2019-03-14T22:00:00.000Z",  
      "NotBefore": "2019-03-14T20:00:00.000Z",  
      "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"  
    }  
  ]  
]
```

Actions pour le redémarrage d'une instance

Vous pouvez attendre que le redémarrage d'instance se produise dans sa fenêtre de maintenance planifiée, [reprogrammer](#) le redémarrage d'instance à une date et heure qui vous conviennent, ou [redémarrer](#) vous-même l'instance au moment qui vous convient.

Après le redémarrage de votre instance, l'événement planifié pour le redémarrage d'instance est annulé et la description de l'événement est mise à jour. La maintenance en attente pour l'hôte sous-jacent est effectuée et vous pouvez recommencer à utiliser votre instance après son démarrage complet.

Actions pour le redémarrage du système

Vous ne pouvez pas redémarrer le système vous-même. Vous pouvez attendre que le redémarrage de système se produise dans sa fenêtre de maintenance planifiée, ou vous pouvez [reprogrammer](#) le redémarrage de système à une date et heure qui vous conviennent. Un redémarrage de système se

termine généralement en quelques minutes. Une fois le redémarrage du système effectué, l'instance conserve son adresse IP et son nom DNS, et les données sur les volumes de stockage d'instance locaux sont conservées. Une fois le redémarrage du système achevé, l'événement planifié pour l'instance est effacé et vous pouvez vérifier que les logiciels sur votre instance fonctionnent comme prévu.

Sinon, s'il est nécessaire d'intervenir sur l'instance à un autre moment et que vous ne pouvez pas reprogrammer le redémarrage du système, vous pouvez arrêter et démarrer une instance basée sur les volumes Amazon EBS, ce qui la migre vers un nouvel hôte. Par contre, les données sur les volumes de stockage d'instance locaux ne sont pas conservées. Vous pouvez également automatiser un arrêt d'instance immédiat et un démarrage en réponse à un événement planifié de réinitialisation du système. Pour plus d'informations, consultez [Actions d'automatisation pour des instances EC2](#) dans le AWS Health Guide de l'utilisateur. Dans le cas d'une instance basée sur le stockage d'instance, si vous ne pouvez pas reprogrammer le redémarrage de système, vous pouvez alors lancer une instance de remplacement à partir de votre AMI la plus récente, migrer toutes les données nécessaires vers l'instance de remplacement avant la fenêtre de maintenance planifiée, puis mettre fin à l'instance d'origine.

Gérer les instances planifiées pour une maintenance

Lorsqu' AWS il doit gérer l'hôte sous-jacent d'une instance, il planifie la maintenance de l'instance. Il existe deux types d'événements de maintenance : maintenance du réseau et maintenance de l'alimentation.

Lors d'une maintenance du réseau, les instances planifiées perdent leur connectivité réseau pendant une courte période. La connectivité réseau normale vers votre instance est restaurée une fois la maintenance terminée.

Lors d'une maintenance de l'alimentation, les instances planifiées sont mises hors ligne pendant une courte période, puis redémarrées. Lorsqu'un redémarrage est effectué, les paramètres de configuration de votre instance sont conservés.

Une fois que votre instance a redémarré (cela prend normalement quelques minutes), vérifiez que votre application fonctionne comme prévu. À ce stade, votre instance ne devrait plus avoir d'événement planifié associé. Dans le cas contraire, la description de l'événement planifié commence par [Terminé]. Cela peut parfois prendre jusqu'à 1 heure pour que la description de statut de cette instance soit actualisée. Les événements de maintenance terminés restent affichés sur le tableau de bord de la console Amazon EC2 pendant une semaine maximum.

Actions pour les instances basées sur Amazon EBS

Vous pouvez attendre que la maintenance ait lieu comme planifié. Sinon, vous pouvez arrêter et démarrer l'instance, ce qui la migre vers un nouvel hôte. Pour plus d'informations sur l'arrêt de votre instance, ainsi que des informations sur les changements apportés à la configuration de votre instance lorsque celle-ci est arrêtée, consultez [Arrêtez et démarrez les instances Amazon EC2](#).

Vous pouvez automatiser un arrêt immédiat et un démarrage en réponse à un événement planifié de maintenance. Pour plus d'informations, consultez [Actions d'automatisation pour des instances EC2](#) dans le AWS Health Guide de l'utilisateur.

Actions pour les instances basées sur le stockage d'instance

Vous pouvez attendre que la maintenance ait lieu comme planifié. Sinon, si vous souhaitez conserver un fonctionnement normal pendant une fenêtre de maintenance planifiée, vous pouvez lancer une instance de remplacement à partir de votre AMI la plus récente, migrer toutes les données nécessaires vers l'instance de remplacement avant la fenêtre de maintenance planifiée, puis mettre fin à l'instance d'origine.

Replanifier un événement planifié

Vous pouvez replanifier un événement de sorte qu'il se produise à une date et une heure spécifiques qui vous conviennent. Seuls les événements ayant une date d'échéance peuvent être reprogrammés. Il existe d'autres [restrictions pour la reprogrammation d'un événement](#).

Vous pouvez replanifier un événement à l'aide de l'une des méthodes suivantes.

Console

Pour replanifier un événement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Type de ressource : instance dans la liste des filtres.
4. Sélectionnez une ou plusieurs instances, puis sélectionnez Actions, Schedule Event (Programmer un événement).

Seuls les événements ayant une date d'échéance, indiquée par la valeur Event Deadline (Échéance de l'événement), peuvent être reprogrammés. Si l'un des événements sélectionnés n'a pas de date d'échéance, Actions, Schedule Event (Programmer un événement) est désactivé.

5. Dans **New start time** (Nouvelle heure de début), saisissez une nouvelle date et une nouvelle heure pour l'événement. La nouvelle date et la nouvelle heure doivent être antérieures à la valeur de **Event Deadline** (Échéance de l'événement).
6. Choisissez **Enregistrer**.

L'heure de démarrage mise à jour peut prendre une à deux minutes pour s'afficher dans la console.

AWS CLI

Pour replanifier un événement

1. Seuls les événements dotés d'une date d'échéance d'événement, indiquée par la valeur pour **NotBeforeDeadline**, peuvent être reprogrammés. Utilisez la commande [describe-instance-status](#) pour afficher la valeur de paramètre **NotBeforeDeadline**.

```
aws ec2 describe-instance-status \  
  --instance-id i-1234567890abcdef0
```

L'exemple de sortie suivant illustre un événement **system-reboot** qui peut être reprogrammé, car **NotBeforeDeadline** contient une valeur.

```
[  
  "Events": [  
    {  
      "InstanceEventId": "instance-event-0d59937288b749b32",  
      "Code": "system-reboot",  
      "Description": "The instance is scheduled for a reboot",  
      "NotAfter": "2019-03-14T22:00:00.000Z",  
      "NotBefore": "2019-03-14T20:00:00.000Z",  
      "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"  
    }  
  ]  
]
```

2. Pour reprogrammer l'événement, utilisez la commande [modify-instance-event-start-time](#). Spécifiez la nouvelle heure de début de l'événement à l'aide du paramètre **not-before**. La nouvelle heure de début doit se situer avant la **NotBeforeDeadline**.

```
aws ec2 modify-instance-event-start-time \  
  --not-before
```

```
--instance-id i-1234567890abcdef0 \  
--instance-event-id instance-event-0d59937288b749b32 \  
--not-before 2019-03-25T10:00:00.000
```

Cela peut prendre une à deux minutes pour que la commande [describe-instance-status](#) renvoie la valeur de paramètre `not-before` mise à jour.

Limites

- Seuls les événements dotés d'une date d'échéance d'événement peuvent être reprogrammés. L'événement peut être reprogrammé jusqu'à la date d'échéance de celui-ci. La colonne Date limite de la console et le `NotBeforeDeadline` champ de la colonne AWS CLI indiquent si l'événement a une date limite.
- Seuls les événements n'ayant pas encore démarré peuvent être reprogrammés. La colonne Heure de début de la console et le `NotBefore` champ de la AWS CLI indiquent l'heure de début de l'événement. Les événements programmés pour un lancement dans les 5 prochaines minutes ne peuvent pas être reprogrammés.
- La nouvelle heure de début doit être au moins 60 minutes après l'heure actuelle.
- Si vous reprogrammez plusieurs événements à l'aide de la console, la date d'échéance de l'événement est déterminée par l'événement avec la date d'échéance d'événement la plus proche.

Définir des fenêtres d'événements pour des événements planifiés

Vous pouvez définir des fenêtres d'événements hebdomadaires personnalisées récurrentes pour des événements planifiés qui redémarrent, arrêtent ou résilient vos instances Amazon EC2. Vous pouvez associer une ou plusieurs instances à une fenêtre d'événements. Si un événement est planifié pour ces instances, AWS planifiera les événements dans la fenêtre d'événements associée.

Vous pouvez utiliser des fenêtres d'événements afin d'optimiser la disponibilité de la charge de travail globale en spécifiant des fenêtres d'événements pendant des périodes creuses pour cette charge de travail. Vous pouvez également aligner les fenêtres d'événements avec vos planifications de maintenance internes.

Vous définissez une fenêtre d'événements en spécifiant un ensemble de plages de temps. La plage de temps minimale est de 2 heures. Les plages de temps combinées doivent totaliser au moins 4 heures.

Vous pouvez associer une ou plusieurs instances à une fenêtre d'événements en utilisant des ID d'instance ou des étiquettes d'instance. Vous pouvez également associer des hôtes dédiés à une fenêtre d'événements en utilisant l'ID d'hôte.

 Warning

Les fenêtres d'événements s'appliquent uniquement à des événements planifiés qui arrêtent, redémarrent ou résilient des instances.

Les fenêtres d'événements ne sont pas applicables aux événements suivants :

- Événements planifiés accélérés et événements de maintenance du réseau.
- Maintenance imprévue, telle que AutoRecovery redémarrages imprévus.

Utiliser les fenêtres d'événements

- [Considérations](#)
- [Afficher les fenêtres d'événements](#)
- [Créer des fenêtres d'événements](#)
- [Modifier des fenêtres d'événements](#)
- [Supprimer des fenêtres d'événements](#)
- [Etiqueter des fenêtres d'événements](#)

Considérations

- Toutes les heures de fenêtre d'événements sont au format UTC.
- La durée minimale d'une fenêtre d'événements hebdomadaire est de 4 heures.
- Les plages de temps au sein d'une fenêtre d'événements doivent être d'au moins 2 heures chacune.
- Un seul type de cible (ID d'instance, ID d'hôte dédié ou étiquette d'instance) peut être associé à une fenêtre d'événements.
- Une cible (ID d'instance, ID d'hôte dédié ou étiquette d'instance) ne peut être associée qu'à à une fenêtre d'événements.
- Au maximum 100 ID d'instance, 50 ID d'hôte dédié ou 50 étiquettes d'instance peuvent être associés à une fenêtre d'événements. Les étiquettes d'instance peuvent être associées à un nombre quelconque d'instances.

- Un maximum de 200 fenêtres d'événements peuvent être créées par AWS région.
- Plusieurs instances associées à des fenêtres d'événements peuvent avoir des événements planifiés se produisant en même temps.
- Si vous avez AWS déjà planifié un événement, la modification d'une fenêtre d'événements ne changera pas l'heure de l'événement planifié. Si l'événement a une date d'échéance, vous pouvez [replanifier l'événement](#).
- Vous pouvez arrêter et démarrer une instance avant l'événement planifié. Cela a pour effet de migrer l'instance vers un nouvel hôte, de sorte que l'événement planifié n'aura plus lieu.

Afficher les fenêtres d'événements

Vous pouvez afficher les fenêtres d'événements à l'aide de l'une des méthodes suivantes.

Console

Pour afficher les fenêtres d'événements

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Sélectionnez une fenêtre d'événements pour voir ses détails.

AWS CLI

Pour décrire toutes les fenêtres d'événements

Utilisez la commande [describe-instance-event-windows](#).

```
aws ec2 describe-instance-event-windows \  
  --region us-east-1
```

Sortie attendue

```
{  
  "InstanceEventWindows": [  
    {  
      "InstanceEventWindowId": "iew-0abcdef1234567890",  
      "Name": "myEventWindowName",
```

```
    "CronExpression": "* 21-23 * * 2,3",
    "AssociationTarget": {
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-0598c7d356eba48d7"
      ],
      "Tags": [],
      "DedicatedHostIds": []
    },
    "State": "active",
    "Tags": []
  }

  ...

],
"NextToken": "9d624e0c-388b-4862-a31e-a85c64fc1d4a"
}
```

Pour décrire une fenêtre d'événements spécifique

Utilisez la commande [describe-instance-event-windows](#) avec le paramètre `--instance-event-window-id` pour décrire une fenêtre d'événements spécifique.

```
aws ec2 describe-instance-event-windows \
  --region us-east-1 \
  --instance-event-window-id iew-0abcdef1234567890
```

Pour décrire des fenêtres d'événements correspondant à un ou plusieurs filtres

Utilisez la commande [describe-instance-event-windows](#) avec le paramètre `--filters`. Dans l'exemple suivant, le filtre `instance-id` est utilisé pour décrire toutes les fenêtres d'événements associées à l'instance spécifiée.

Quand un filtre est utilisé, il recherche une correspondance directe. Cependant, le filtre `instance-id` est différent. À défaut de correspondance directe avec l'ID d'instance, il recherche des associations indirectes avec la fenêtre d'événements, telles que les étiquettes ou l'ID d'hôte dédié de l'instance (si celle-ci se trouve sur un hôte dédié).

Pour obtenir la liste des filtres pris en charge, consultez [describe-instance-event-windows](#) dans la AWS CLI Référence.

```
aws ec2 describe-instance-event-windows \  
  --region us-east-1 \  
  --filters Name=instance-id,Values=i-1234567890abcdef0 \  
  --max-results 100 \  
  --next-token <next-token-value>
```

Sortie attendue

Dans l'exemple suivant, l'instance se trouve sur un hôte dédié qui est associé à la fenêtre d'événements.

```
{  
  "InstanceEventWindows": [  
    {  
      "InstanceEventWindowId": "iew-0dbc0adb66f235982",  
      "TimeRanges": [  
        {  
          "StartWeekDay": "sunday",  
          "StartHour": 2,  
          "EndWeekDay": "sunday",  
          "EndHour": 8  
        }  
      ],  
      "Name": "myEventWindowName",  
      "AssociationTarget": {  
        "InstanceIds": [],  
        "Tags": [],  
        "DedicatedHostIds": [  
          "h-0140d9a7ecbd102dd"  
        ]  
      },  
      "State": "active",  
      "Tags": []  
    }  
  ]  
}
```

Créer des fenêtres d'événements

Vous pouvez créer une ou plusieurs fenêtres d'événements. Pour chaque fenêtre d'événements, vous spécifiez un ou plusieurs blocs de temps. Par exemple, vous pouvez créer une fenêtre

d'événements avec des blocs de temps qui se produisent tous les jours à 4 heures du matin pendant 2 heures. Ou vous pouvez créer une fenêtre d'événements avec des blocs de temps qui se produisent les dimanches de 2 à 4 heures et les mercredis de 3 à 5 heures.

Pour connaître les contraintes de fenêtre d'événements, consultez [Considérations](#) plus haut dans cette rubrique.

Les fenêtres d'événements se reproduisent à une fréquence hebdomadaire jusqu'à ce que vous les supprimiez.

Pour créer une fenêtre d'événements, utilisez l'une des méthodes suivantes.

Console

Pour créer une fenêtre d'événements

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Choisissez Créer une fenêtre d'événements d'instance.
5. Pour Nom de la fenêtre d'événements, saisissez un nom descriptif.
6. Pour Planification de la fenêtre d'événements, choisissez de spécifier les blocs de temps dans la fenêtre d'événements à l'aide du générateur de planification cron ou en spécifiant des plages de temps.
 - Si vous choisissez Générateur de planification Cron, spécifiez les paramètres suivants :
 1. Pour Jours (UTC), spécifiez les jours de la semaine où la fenêtre d'événements se produit.
 2. Pour Heure de début (UTC), spécifiez l'heure à laquelle la fenêtre d'événements commence.
 3. Pour Durée, spécifiez la durée des blocs de temps dans la fenêtre d'événements. La durée minimale par bloc de temps est de 2 heures. La durée minimale de la fenêtre d'événements doit être égale ou supérieure à 4 heures au total. Toutes les heures sont indiquées en heure universelle coordonnée (UTC).
 - Si vous choisissez Plages de temps, choisissez Ajouter une nouvelle plage de temps, puis spécifiez le jour et l'heure de début, ainsi que le jour et l'heure de fin. Répétez l'opération pour chaque plage de temps. La durée minimale par plage de temps est de 2 heures. La

durée minimale pour toutes les plages de temps combinées doit être égale ou supérieure à 4 heures au total.

7. (Facultatif) Pour Détails de la cible, associez une ou plusieurs instances à la fenêtre d'événements afin que, si les instances sont planifiées pour maintenance, l'événement planifié se produise durant la fenêtre d'événement associée. Vous pouvez associer une ou plusieurs instances avec une fenêtre d'événements à l'aide d'ID d'instance ou d'étiquettes d'instance. Vous pouvez associer des hôtes dédiés avec une fenêtre d'événements en utilisant l'ID d'hôte.

Notez que vous pouvez créer la fenêtre d'événements sans y associer de cible. Plus tard, vous pourrez modifier la fenêtre pour associer une ou plusieurs cibles.

8. (Facultatif) Pour Etiquettes de la fenêtre d'événements, choisissez Ajouter une étiquette, puis saisissez la clé et la valeur de l'étiquette. Répétez l'opération pour chaque étiquette.
9. Choisissez Créer une fenêtre d'événements.

AWS CLI

Pour créer une fenêtre d'événements à l'aide de AWS CLI, vous devez d'abord créer la fenêtre d'événements, puis vous associez une ou plusieurs cibles à la fenêtre d'événements.

Créer une fenêtre d'événements

Lors de la création de la fenêtre d'événements, vous pouvez définir un ensemble de plages de temps ou une expression cron, mais pas les deux.

Pour créer une fenêtre d'événements avec une plage de temps

Utilisez la commande [create-instance-event-window](#) avec le paramètre `--time-range`. Vous ne pouvez pas également spécifier le paramètre `--cron-expression`.

```
aws ec2 create-instance-event-window \  
  --region us-east-1 \  
  --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \  
  --tag-specifications "ResourceType=instance-event-  
window,Tags=[{Key=K1,Value=V1}]" \  
  --name myEventWindowName
```

Sortie attendue

```
{
```

```

"InstanceEventWindow": {
  "InstanceEventWindowId": "iew-0abcdef1234567890",
  "TimeRanges": [
    {
      "StartWeekDay": "monday",
      "StartHour": 2,
      "EndWeekDay": "wednesday",
      "EndHour": 8
    }
  ],
  "Name": "myEventWindowName",
  "State": "creating",
  "Tags": [
    {
      "Key": "K1",
      "Value": "V1"
    }
  ]
}

```

Pour créer une fenêtre d'événements avec une expression cron à

Utilisez la commande [create-instance-event-window](#) avec le paramètre `--cron-expression`. Vous ne pouvez pas également spécifier le paramètre `--time-range`.

```

aws ec2 create-instance-event-window \
  --region us-east-1 \
  --cron-expression "* 21-23 * * 2,3" \
  --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
  --name myEventWindowName

```

Sortie attendue

```

{
  "InstanceEventWindow": {
    "InstanceEventWindowId": "iew-0abcdef1234567890",
    "Name": "myEventWindowName",
    "CronExpression": "* 21-23 * * 2,3",
    "State": "creating",
    "Tags": [
      {

```

```

        "Key": "K1",
        "Value": "V1"
      }
    ]
  }
}

```

Associer une cible à une fenêtre d'événements

Vous ne pouvez associer qu'un seul type de cible (ID d'instance, ID d'hôte dédié ou étiquette d'instance) à une fenêtre d'événements.

Pour associer des étiquettes d'instance à une fenêtre d'événements

Utilisez la commande [associate-instance-event-window](#) avec le paramètre `instance-event-window-id` pour spécifier la fenêtre d'événements. Pour associer des étiquettes d'instance, spécifiez le paramètre `--association-target`, et pour les valeurs de paramètre, spécifiez une ou plusieurs étiquettes.

```

aws ec2 associate-instance-event-window \
  --region us-east-1 \
  --instance-event-window-id iew-0abcdef1234567890 \
  --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"

```

Sortie attendue

```

{
  "InstanceEventWindow": {
    "InstanceEventWindowId": "iew-0abcdef1234567890",
    "Name": "myEventWindowName",
    "CronExpression": "* 21-23 * * 2,3",
    "AssociationTarget": {
      "InstanceIds": [],
      "Tags": [
        {
          "Key": "k2",
          "Value": "v2"
        },
        {
          "Key": "k1",
          "Value": "v1"
        }
      ]
    }
  }
}

```

```

    ],
    "DedicatedHostIds": []
  },
  "State": "creating"
}
}

```

Pour associer une ou plusieurs instances à une fenêtre d'événements

Utilisez la commande [associate-instance-event-window](#) avec le paramètre `instance-event-window-id` pour spécifier la fenêtre d'événements. Pour associer des instances, spécifiez le paramètre `--association-target`, et pour les valeurs de paramètre, spécifiez un ou plusieurs ID d'instance.

```

aws ec2 associate-instance-event-window \
  --region us-east-1 \
  --instance-event-window-id iew-0abcdef1234567890 \
  --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"

```

Sortie attendue

```

{
  "InstanceEventWindow": {
    "InstanceEventWindowId": "iew-0abcdef1234567890",
    "Name": "myEventWindowName",
    "CronExpression": "* 21-23 * * 2,3",
    "AssociationTarget": {
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-0598c7d356eba48d7"
      ],
      "Tags": [],
      "DedicatedHostIds": []
    },
    "State": "creating"
  }
}

```

Pour associer un hôte dédié à une fenêtre d'événements

Utilisez la commande [associate-instance-event-window](#) avec le paramètre `instance-event-window-id` pour spécifier la fenêtre d'événements. Pour associer un hôte dédié, spécifiez le

paramètre `--association-target`, et pour les valeurs de paramètre, spécifiez un ou plusieurs ID d'hôte dédié.

```
aws ec2 associate-instance-event-window \  
  --region us-east-1 \  
  --instance-event-window-id iew-0abcdef1234567890 \  
  --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Sortie attendue

```
{  
  "InstanceEventWindow": {  
    "InstanceEventWindowId": "iew-0abcdef1234567890",  
    "Name": "myEventWindowName",  
    "CronExpression": "* 21-23 * * 2,3",  
    "AssociationTarget": {  
      "InstanceIds": [],  
      "Tags": [],  
      "DedicatedHostIds": [  
        "h-029fa35a02b99801d"  
      ]  
    },  
    "State": "creating"  
  }  
}
```

Modifier des fenêtres d'événements

Vous pouvez modifier tous les champs d'une fenêtre d'événements à l'exception de son ID. Par exemple, quand l'heure d'été commence, vous pouvez modifier la planification de la fenêtre d'événements. Pour des fenêtres d'événements existantes, vous pouvez ajouter ou supprimer des cibles.

Pour modifier une fenêtre d'événements, utilisez l'une des méthodes suivantes.

Console

Pour modifier une fenêtre d'événements

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Événements.

3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Sélectionnez la fenêtre d'événements à modifier, puis choisissez Actions, Modifier la fenêtre d'événements d'instance.
5. Modifiez les champs de la fenêtre d'événements, puis choisissez Modifier la fenêtre d'événements.

AWS CLI

Pour modifier une fenêtre d'événements à l'aide de AWS CLI, vous pouvez modifier la plage de temps ou l'expression cron, et associer ou dissocier une ou plusieurs cibles à la fenêtre d'événements.

Modifier l'heure de la fenêtre d'événements

Lors de la modification de la fenêtre d'événements, vous pouvez modifier une plage de temps ou une expression cron, mais pas les deux.

Pour modifier la plage de temps d'une fenêtre d'événements

Utilisez la commande [modify-instance-event-window](#) et spécifiez la fenêtre d'événements à modifier. Spécifiez le paramètre `--time-range` pour modifier la plage de temps. Vous ne pouvez pas également spécifier le paramètre `--cron-expression`.

```
aws ec2 modify-instance-event-window \  
  --region us-east-1 \  
  --instance-event-window-id iew-0abcdef1234567890 \  
  --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Sortie attendue

```
{  
  "InstanceEventWindow": {  
    "InstanceEventWindowId": "iew-0abcdef1234567890",  
    "TimeRanges": [  
      {  
        "StartWeekDay": "monday",  
        "StartHour": 2,  
        "EndWeekDay": "wednesday",  
        "EndHour": 8  
      }  
    ],  
  },  
}
```

```

    "Name": "myEventWindowName",
    "AssociationTarget": {
      "InstanceIds": [
        "i-0abcdef1234567890",
        "i-0be35f9acb8ba01f0"
      ],
      "Tags": [],
      "DedicatedHostIds": []
    },
    "State": "creating",
    "Tags": [
      {
        "Key": "K1",
        "Value": "V1"
      }
    ]
  }
}

```

Pour modifier une ensemble de plages de temps pour une fenêtre d'événements

Utilisez la commande [modify-instance-event-window](#) et spécifiez la fenêtre d'événements à modifier. Spécifiez le paramètre `--time-range` pour modifier la plage de temps. Vous ne pouvez pas spécifier également le paramètre `--cron-expression` dans le même appel.

```

aws ec2 modify-instance-event-window \
  --region us-east-1 \
  --instance-event-window-id iew-0abcdef1234567890 \
  --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay": "wednesday", "EndHour": 8}, {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday", "EndHour": 8}]'

```

Sortie attendue

```

{
  "InstanceEventWindow": {
    "InstanceEventWindowId": "iew-0abcdef1234567890",
    "TimeRanges": [
      {
        "StartWeekDay": "monday",
        "StartHour": 2,
        "EndWeekDay": "wednesday",

```

```

        "EndHour": 8
      },
      {
        "StartWeekDay": "thursday",
        "StartHour": 2,
        "EndWeekDay": "friday",
        "EndHour": 8
      }
    ],
    "Name": "myEventWindowName",
    "AssociationTarget": {
      "InstanceIds": [
        "i-0abcdef1234567890",
        "i-0be35f9acb8ba01f0"
      ],
      "Tags": [],
      "DedicatedHostIds": []
    },
    "State": "creating",
    "Tags": [
      {
        "Key": "K1",
        "Value": "V1"
      }
    ]
  }
}

```

Pour modifier l'expression cron d'une fenêtre d'événements

Utilisez la commande [modify-instance-event-window](#) et spécifiez la fenêtre d'événements à modifier. Spécifiez le paramètre `--cron-expression` pour modifier l'expression cron. Vous ne pouvez pas également spécifier le paramètre `--time-range`.

```

aws ec2 modify-instance-event-window \
  --region us-east-1 \
  --instance-event-window-id iew-0abcdef1234567890 \
  --cron-expression "* 21-23 * * 2,3"

```

Sortie attendue

```

{
  "InstanceEventWindow": {

```

```
"InstanceEventWindowId": "iew-0abcdef1234567890",
  "Name": "myEventWindowName",
  "CronExpression": "* 21-23 * * 2,3",
  "AssociationTarget": {
    "InstanceIds": [
      "i-0abcdef1234567890",
      "i-0be35f9acb8ba01f0"
    ],
    "Tags": [],
    "DedicatedHostIds": []
  },
  "State": "creating",
  "Tags": [
    {
      "Key": "K1",
      "Value": "V1"
    }
  ]
}
```

Modifier les cibles associées à une fenêtre d'événements

Vous pouvez associer des cibles supplémentaires à une fenêtre d'événements. Vous pouvez également dissocier des cibles existantes d'une fenêtre d'événements. Toutefois, vous ne pouvez associer qu'un seul type de cible (ID d'instance, ID d'hôte dédié ou étiquette d'instance) à une fenêtre d'événements.

Pour associer des cibles supplémentaires à une fenêtre d'événements

Pour obtenir des instructions sur la façon d'associer des cibles à une fenêtre d'événements, consultez [Associate a target with an event window](#).

Pour dissocier des étiquettes d'instance d'une fenêtre d'événements

Utilisez la commande [disassociate-instance-event-window](#) avec le paramètre `instance-event-window-id` pour spécifier la fenêtre d'événements. Pour dissocier des étiquettes d'instance, spécifiez le paramètre `--association-target`, et pour les valeurs de paramètre, spécifiez une ou plusieurs étiquettes.

```
aws ec2 disassociate-instance-event-window \
  --region us-east-1 \
  --instance-event-window-id iew-0abcdef1234567890 \
```

```
--association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Sortie attendue

```
{
  "InstanceEventWindow": {
    "InstanceEventWindowId": "iew-0abcdef1234567890",
    "Name": "myEventWindowName",
    "CronExpression": "* 21-23 * * 2,3",
    "AssociationTarget": {
      "InstanceIds": [],
      "Tags": [],
      "DedicatedHostIds": []
    },
    "State": "creating"
  }
}
```

Pour dissocier une ou plusieurs instances d'une fenêtre d'événements

Utilisez la commande [disassociate-instance-event-window](#) avec le paramètre `instance-event-window-id` pour spécifier la fenêtre d'événements. Pour dissocier des instances, spécifiez le paramètre `--association-target`, et pour les valeurs de paramètre, spécifiez un ou plusieurs ID d'instance.

```
aws ec2 disassociate-instance-event-window \
  --region us-east-1 \
  --instance-event-window-id iew-0abcdef1234567890 \
  --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Sortie attendue

```
{
  "InstanceEventWindow": {
    "InstanceEventWindowId": "iew-0abcdef1234567890",
    "Name": "myEventWindowName",
    "CronExpression": "* 21-23 * * 2,3",
    "AssociationTarget": {
      "InstanceIds": [],
      "Tags": [],
      "DedicatedHostIds": []
    },
  },
}
```

```
    "State": "creating"
  }
}
```

Pour dissocier un hôte dédié d'une fenêtre d'événements

Utilisez la commande [disassociate-instance-event-window](#) avec le paramètre `instance-event-window-id` pour spécifier la fenêtre d'événements. Pour dissocier un hôte dédié, spécifiez le paramètre `--association-target`, et pour les valeurs de paramètre, spécifiez un ou plusieurs ID d'hôte dédié.

```
aws ec2 disassociate-instance-event-window \
  --region us-east-1 \
  --instance-event-window-id iew-0abcdef1234567890 \
  --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Sortie attendue

```
{
  "InstanceEventWindow": {
    "InstanceEventWindowId": "iew-0abcdef1234567890",
    "Name": "myEventWindowName",
    "CronExpression": "* 21-23 * * 2,3",
    "AssociationTarget": {
      "InstanceIds": [],
      "Tags": [],
      "DedicatedHostIds": []
    },
    "State": "creating"
  }
}
```

Supprimer des fenêtres d'événements

Vous pouvez supprimer une fenêtre d'événements à la fois à l'aide de l'une des méthodes suivantes.

Console

Pour supprimer une fenêtre d'événements

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Sélectionnez la fenêtre d'événements à supprimer, puis choisissez Actions, Supprimer la fenêtre d'événements d'instance.
5. Lorsque vous y êtes invité, tapez **delete**, puis choisissez Supprimer.

AWS CLI

Pour supprimer une fenêtre d'événements

Utilisez la commande [delete-instance-event-window](#) et spécifiez la fenêtre d'événements à supprimer.

```
aws ec2 delete-instance-event-window \  
  --region us-east-1 \  
  --instance-event-window-id iew-0abcdef1234567890
```

Pour supprimer de force une fenêtre d'événements

Utilisez le paramètre `--force-delete` si la fenêtre d'événements est actuellement associée à des cibles.

```
aws ec2 delete-instance-event-window \  
  --region us-east-1 \  
  --instance-event-window-id iew-0abcdef1234567890 \  
  --force-delete
```

Sortie attendue

```
{  
  "InstanceEventWindowState": {  
    "InstanceEventWindowId": "iew-0abcdef1234567890",  
    "State": "deleting"  
  }  
}
```

Étiqueter des fenêtres d'événements

Vous pouvez étiqueter une fenêtre d'événements lorsque vous la créez, ou ultérieurement.

Pour étiqueter une fenêtre d'événements lorsque vous la créez, consultez [Créer des fenêtres d'événements](#).

Pour étiqueter une fenêtre d'événements, utilisez l'une des méthodes suivantes.

Console

Pour étiqueter une fenêtre d'événements existante

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Événements.
3. Choisissez Actions, Gérer les fenêtres d'événements.
4. Sélectionnez la fenêtre d'événements à étiqueter, puis choisissez Actions, Etiqueter la fenêtre d'événements d'instance.
5. Pour ajouter une étiquette, choisissez Ajouter une étiquette. Répétez l'opération pour chaque étiquette.
6. Choisissez Enregistrer.

AWS CLI

Pour étiqueter une fenêtre d'événements existante

Utilisez la commande [create-tags](#) pour baliser les ressources existantes. Dans l'exemple suivant, la fenêtre d'événements existante est étiquetée avec Key=purpose et Value=test.

```
aws ec2 create-tags \  
  --resources iew-0abcdef1234567890 \  
  --tags Key=purpose,Value=test
```

Surveillez vos instances à l'aide de CloudWatch

Vous pouvez surveiller vos instances à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes d'Amazon EC2 pour en faire des métriques lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois et, par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute.

Par défaut, Amazon EC2 envoie des données métriques par intervalles de CloudWatch 5 minutes. Pour envoyer les données métriques de votre instance par périodes CloudWatch d'une minute, vous pouvez activer la surveillance détaillée de l'instance. Pour plus d'informations, consultez [Activer ou désactiver la surveillance détaillée pour vos instances](#).

La console Amazon EC2 affiche une série de graphiques basés sur les données brutes d'Amazon CloudWatch. Selon vos besoins, vous préférez peut-être obtenir les données de vos instances auprès d'Amazon CloudWatch plutôt que de consulter les graphiques de la console.

Pour obtenir des informations sur la CloudWatch facturation et les coûts d'Amazon, consultez la section [CloudWatch facturation et coûts](#) dans le guide de CloudWatch l'utilisateur Amazon.

Table des matières

- [Alarmes relatives aux instances Amazon EC2](#)
- [Activer ou désactiver la surveillance détaillée pour vos instances](#)
- [Répertoriez CloudWatch les métriques disponibles pour vos instances](#)
- [Installez et configurez l' CloudWatchagent à l'aide de la console Amazon EC2 pour ajouter des métriques supplémentaires](#)
- [Obtenir les statistiques des métriques de vos instances](#)
- [Représenter graphiquement les métriques de vos instances](#)
- [Création d'une CloudWatch alarme pour une instance](#)
- [Créer des alarmes qui arrêtent, finissent, redémarrent ou récupèrent une instance](#)

Alarmes relatives aux instances Amazon EC2

Vous pouvez afficher et créer des CloudWatch alarmes Amazon pour vos instances depuis l'écran Instances de la console Amazon EC2.

La capture d'écran suivante indique les commandes de console, numérotées 1 et 2, permettant de visualiser et de créer des alarmes à partir de l'écran Instances.

Instances (7) Info

Find Instance by attribute or tag (case-sensitive) All states ▾

<input type="checkbox"/>	Name 	Instance ID	Instance state 	Instance type 	Status check	Alarm status
<input type="checkbox"/>	My-1-Spot-Ins...	I-01aeed690c9fb5322	 Running  	t3.nano	 2/2 checks passed	 1 View alarms 
<input type="checkbox"/>	My-2-Spot-Ins...	I-0ba5e5bbc9d634fa6	 Stopped  	t3.nano	-	View alarm 2 

Afficher les alarmes depuis l'écran Instances

Vous pouvez consulter les alarmes de chaque instance depuis l'écran Instances.

Pour afficher l'alarme d'une instance depuis l'écran Instances

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Dans le tableau Instances, pour l'instance que vous avez choisie, choisissez Afficher les alarmes (numérotée 1 dans la capture d'écran précédente).
4. Dans la fenêtre Détails de l'alarme pour ***i-0123456789example***, choisissez le nom de l'alarme pour afficher l'alarme dans la console. CloudWatch

Créer des alarmes à partir de l'écran Instances

Vous pouvez créer une alarme pour chaque instance à partir de l'écran Instances.

Pour créer une alarme pour une instance à partir de l'écran Instances

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Dans le tableau Instances, pour l'instance que vous avez choisie, choisissez le signe plus (numéroté 2 dans la capture d'écran précédente).
4. Dans l'écran Gérer les CloudWatch alarmes, créez votre alarme. Pour plus d'informations, consultez [Création d'une CloudWatch alarme pour une instance](#).

Activer ou désactiver la surveillance détaillée pour vos instances

Par défaut, la surveillance basique est activée pour votre instance, mais vous pouvez activer la surveillance détaillée si vous le souhaitez.

Le tableau suivant met en évidence les différences entre la surveillance de base et la surveillance détaillée des instances.

Type de surveillance	Description	Frais
Surveillance de base	<p>Seules les métriques de contrôle de statut sont disponibles par périodes d'une minute.</p> <p>Toutes les autres métriques sont disponibles par périodes de cinq minutes.</p>	Aucuns frais.
Surveillance détaillée	<p>Toutes les métriques, y compris les métriques de contrôle de statut, sont disponibles par périodes d'une minute. Pour obtenir le niveau de données, vous devez l'activer spécifiquement pour l'instance. Pour les instances où vous avez activé la surveillance détaillée, vous pouvez également obtenir les données agrégées à partir de groupes d'instances similaires.</p>	<p>Vous êtes débité par métrique envoyée à CloudWatch. Vous n'êtes pas facturé pour le stockage des données. Pour plus d'informations, consultez le niveau payant et l'exemple 1 - Surveillance détaillée de l'EC2 sur la page de CloudWatch tarification d'Amazon.</p>

Rubriques

- [Autorisations IAM requises](#)
- [Activer la surveillance détaillée](#)
- [Désactiver la surveillance détaillée](#)

Autorisations IAM requises

Pour activer la surveillance détaillée d'une instance, votre utilisateur doit être autorisé à utiliser l'action d'API [MonitorInstances](#). Pour désactiver la surveillance détaillée d'une instance, votre utilisateur doit être autorisé à utiliser l'action d'API [UnmonitorInstances](#).

Activer la surveillance détaillée

Vous pouvez activer la surveillance détaillée sur une instance lors de son lancement, ou une fois qu'elle est en cours d'exécution ou arrêtée. L'activation de la surveillance détaillée d'une instance n'affecte pas la surveillance des volumes EBS attachés à l'instance. Pour plus d'informations, consultez les [CloudWatch métriques Amazon pour Amazon EBS](#).

Console

Pour activer la surveillance détaillée d'une instance existante

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer la surveillance détaillée.
4. Sur la page Surveillance détaillée, pour Surveillance détaillée, sélectionnez la case à cocher Activer.
5. Choisissez Enregistrer.

Pour activer la surveillance détaillée lors du lancement d'une instance

Lorsque vous lancez une instance à l'aide de la console Amazon EC2, sous Détails avancés, cochez la case CloudWatch Surveillance détaillée.

AWS CLI

Pour activer la surveillance détaillée d'une instance existante

Utilisez la commande [monitor-instances](#) suivante pour activer la surveillance détaillée des instances spécifiées.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Pour activer la surveillance détaillée lors du lancement d'une instance

Utilisez la commande [run-instances](#) avec l'indicateur `--monitoring` pour activer la surveillance détaillée.

```
aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

Désactiver la surveillance détaillée

Vous pouvez désactiver la surveillance détaillée sur une instance lors de son lancement, ou une fois qu'elle est en cours d'exécution ou arrêtée.

Console

Pour désactiver la surveillance détaillée

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer la surveillance détaillée.
4. Dans la page Surveillance détaillée, pour Surveillance détaillée, désactivez la case à cocher Activer.
5. Choisissez Enregistrer.

AWS CLI

Pour désactiver la surveillance détaillée

Utilisez la commande [unmonitor-instances](#) suivante pour désactiver la surveillance détaillée des instances spécifiées.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

Répertoriez CloudWatch les métriques disponibles pour vos instances

Amazon EC2 envoie des métriques à Amazon CloudWatch. Vous pouvez utiliser l'API AWS Management Console AWS CLI, le ou une API pour répertorier les métriques auxquelles Amazon EC2 envoie. Par défaut, chaque point de données couvre les 5 minutes suivant l'heure de début d'activité de l'instance. Si vous avez activé la surveillance détaillée, chaque point de données couvre la minute suivant l'activité à compte de l'heure de début. Notez que pour les

statistiques Minimum, Maximum et Moyenne, la granularité minimale des métriques fournies par EC2 est de 1 minute.

Pour plus d'informations sur la façon d'obtenir les statistiques pour ces métriques, consultez [Obtenir les statistiques des métriques de vos instances](#).

Sommaire

- [Métriques des instances](#)
- [Métriques des crédits UC](#)
- [Métriques d'hôte dédié](#)
- [Métriques Amazon EBS pour des instances basées sur Nitro](#)
- [Métriques de contrôle de statut](#)
- [Métriques de mise en miroir du trafic](#)
- [Métriques du groupe Auto Scaling](#)
- [Dimensions de métriques Amazon EC2](#)
- [Métriques d'utilisation Amazon EC2](#)
- [Répertorier les métriques à l'aide de la console](#)
- [Listez les métriques à l'aide du AWS CLI](#)

Métriques des instances

L'espace de nom AWS/EC2 inclut les métriques d'instance suivantes.

Métrique	Description	Unité	Statistiques significatives
CPUUtilization	<p>Le pourcentage de temps de CPU physique qu'Amazon EC2 utilise pour exécuter l'instance EC2, qui comprend le temps passé à exécuter à la fois le code utilisateur et le code Amazon EC2.</p> <p>À un niveau très élevé, CPUUtilization est la somme de l'invité CPUUtilization et de l'hyperviseur CPUUtilization .</p>	Pourcentage	<ul style="list-style-type: none"> • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
	<p>Les outils de votre système d'exploitation peuvent afficher un pourcentage différent de celui CloudWatch dû à des facteurs tels que la simulation d'appareils existants, la configuration d'appareils non existants, les charges de travail nécessitant de nombreuses interruptions, la migration en direct et la mise à jour en direct.</p>		
DiskReadOps	<p>Opérations de lecture terminées de tous les volumes de stockage d'instance disponibles pour l'instance, au cours de la période spécifiée.</p> <p>Pour calculer la moyenne d'opérations d'I/O pour la période, divisez le nombre total d'opérations de la période par le nombre de secondes de la période.</p> <p>S'il n'y a pas de volumes de stockage d'instance, la valeur est 0 ou la métrique n'est pas prise en charge.</p>	Nombre	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum
DiskWriteOps	<p>Opérations d'écriture terminées dans tous les volumes de stockage d'instance disponibles pour l'instance, au cours de la période spécifiée.</p> <p>Pour calculer la moyenne d'opérations d'I/O pour la période, divisez le nombre total d'opérations de la période par le nombre de secondes de la période.</p> <p>S'il n'y a pas de volumes de stockage d'instance, la valeur est 0 ou la métrique n'est pas prise en charge.</p>	Nombre	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
DiskReadBytes	<p>Octets lus à partir de tous les volumes de stockage d'instance disponibles pour l'instance.</p> <p>Cette métrique permet de déterminer le volume de données que l'application lit à partir du disque dur de l'instance. Il est ainsi possible de déterminer la vitesse de l'application.</p> <p>Le nombre mentionné correspond au nombre d'octets reçus pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique <code>DIFF_TIME</code> pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement <code>DiskReadBytes</code> CloudWatch <code>commem1</code>, la formule mathématique de la métrique <code>m1/(DIFF_TIME(m1))</code> renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques <code>DIFF_TIME</code> et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p> <p>S'il n'y a pas de volumes de stockage d'instance, la valeur est 0 ou la métrique n'est pas prise en charge.</p>	Octets	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
DiskWriteBytes	<p>Octets écrits dans tous les volumes de stockage d'instance disponibles pour l'instance.</p> <p>Cette métrique permet de déterminer le volume de données que l'application écrit sur le disque dur de l'instance. Il est ainsi possible de déterminer la vitesse de l'application.</p> <p>Le nombre mentionné correspond au nombre d'octets reçus pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique <code>DIFF_TIME</code> pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement <code>DiskWriteBytes</code> CloudWatch <code>commem1</code>, la formule mathématique de la métrique <code>m1/(DIFF_TIME(m1))</code> renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques <code>DIFF_TIME</code> et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p> <p>S'il n'y a pas de volumes de stockage d'instance, la valeur est 0 ou la métrique n'est pas prise en charge.</p>	Octets	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
MetadataNoToken	<p>Le nombre de fois où le service de métadonnées d'instance (IMDS) a été accédé avec succès à l'aide d'une méthode qui n'utilise pas de jeton.</p> <p>Cette métrique est utilisée pour déterminer s'il existe des processus accédant aux métadonnées d'instance qui utilisent le service de métadonnées d'instance version 1 (IMDSv1), qui n'utilise pas de jeton. Si toutes les demandes utilisent des sessions basées sur des jetons, c'est-à-dire le service de métadonnées d'instance version 2 (IMDSv2), la valeur est 0. Pour plus d'informations, consultez Passer à l'utilisation de Service des métadonnées d'instance Version 2.</p>	Nombre	<ul style="list-style-type: none"> Somme Centiles
MetadataNoTokenRejected	<p>Nombre de tentatives d'appel IMDSv1 après la désactivation d'IMDSv1.</p> <p>Si cette métrique apparaît, elle indique qu'un appel IMDSv1 a été tenté et rejeté. Vous pouvez soit réactiver IMDSv1, soit vous assurer que tous vos appels utilisent IMDSv2. Pour plus d'informations, consultez Passer à l'utilisation de Service des métadonnées d'instance Version 2.</p>	Nombre	<ul style="list-style-type: none"> Somme Centiles

Métrique	Description	Unité	Statistiques significatives
NetworkIn	<p>Nombre d'octets reçus par l'instance sur toutes les interfaces réseau. Cette métrique identifie le volume du trafic réseau entrant d'une seule instance.</p> <p>Le nombre mentionné correspond au nombre d'octets reçus pendant la période. Si vous utilisez une surveillance de base (cinq minutes) et que la statistique est Somme, vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde. Si vous utilisez une surveillance détaillée (une minute) et que la statistique est Somme, divisez-la par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique DIFF_TIME pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement NetworkIn CloudWatch commem1, la formule mathématique de la métrique $m1 / (\text{DIFF_TIME}(m1))$ renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques DIFF_TIME et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p>	Octets	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
NetworkOut	<p>Nombre d'octets envoyés par l'instance sur toutes les interfaces réseau. Cette métrique identifie le volume du trafic réseau sortant d'une seule instance.</p> <p>Le nombre mentionné correspond au nombre d'octets envoyés pendant la période. Si vous utilisez une surveillance de base (cinq minutes) et que la statistique est Somme, vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde. Si vous utilisez une surveillance détaillée (une minute) et que la statistique est Somme, divisez-la par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique DIFF_TIME pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement NetworkOut CloudWatch commem1, la formule mathématique de la métrique $m1 / (\text{DIFF_TIME}(m1))$ renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques DIFF_TIME et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p>	Octets	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
NetworkPacketsIn	<p>Nombre de paquets reçus par l'instance sur toutes les interfaces réseau. Cette métrique identifie le volume du trafic entrant en ce qui concerne le nombre de paquets sur une seule instance.</p> <p>Cette métrique est disponible uniquement pour la surveillance basique (périodes de cinq minutes). Pour calculer le nombre de paquets par seconde (PPS) reçu par votre instance, divisez la valeur statistique Somme par 300. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique <code>DIFF_TIME</code> pour trouver les paquets par seconde. Par exemple, si vous avez représenté graphiquement <code>NetworkPacketsIn</code> CloudWatch comme <code>m1</code>, la formule mathématique de la métrique <code>m1/(DIFF_TIME(m1))</code> renvoie la métrique en paquets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques <code>DIFF_TIME</code> et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p>	Nombre	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
NetworkPacketsOut	<p>Nombre de paquets envoyés par l'instance sur toutes les interfaces réseau. Cette métrique identifie le volume du trafic sortant en ce qui concerne le nombre de paquets sur une seule instance.</p> <p>Cette métrique est disponible uniquement pour la surveillance basique (périodes de cinq minutes). Pour calculer le nombre de paquets par seconde (PPS) envoyé par votre instance en 5 minutes, divisez la valeur statistique Somme par 300. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique DIFF_TIME pour trouver les paquets par seconde. Par exemple, si vous avez représenté graphiquement NetworkPacketsOut CloudWatch commem1, la formule mathématique de la métrique $m1 / (\text{DIFF_TIME}(m1))$ renvoie la métrique en paquets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques DIFF_TIME et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p>	Nombre	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métriques des crédits UC

L'espace de noms AWS/EC2 inclut les métriques de crédit UC suivantes pour vos [instances à capacité extensible](#).

Métrique	Description	Unité	Statistiques significatives
CPUCreditUsage	<p>Nombre de crédits UC dépensés par l'instance pour l'utilisation de l'UC. Par exemple, un crédit UC est équivalent à un processeur virtuel fonctionnant à 100 % d'utilisation pendant une minute ou une combinaison équivalente de processeurs virtuels, d'utilisation et de temps (par exemple, un processeur virtuel fonctionnant à 50 % d'utilisation pendant deux minutes, ou deux processeurs virtuels fonctionnant à 25 % d'utilisation pendant deux minutes).</p> <p>Les métriques de crédits CPU sont disponibles toutes les 5 minutes uniquement. Si vous spécifiez une période supérieure à cinq minutes, utilisez la statistique Sum au lieu de la statistique Average.</p>	Crédits (minutes vCPU)	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum
CPUCreditBalance	<p>Nombre de crédits UC gagnés qu'une instance a accumulés depuis son lancement ou son démarrage. Pour les instances T2 Standard, le CPUCreditBalance inclut également le nombre de crédits de lancement qui ont été accumulés.</p> <p>Les crédits sont accumulés dans le solde de crédits quand ils sont gagnés et supprimés du solde de crédits lorsqu'ils sont dépensés. Le solde de crédits présente une limite maximum qui est déterminée par la taille de l'instance. Une fois que la limite est atteinte, tous les nouveaux crédits gagnés sont rejetés. Pour les instances T2 Standard, les crédits de lancement ne sont pas comptés dans la limite.</p>	Crédits (minutes vCPU)	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
	<p>L'instance peut dépenser les crédits figurant dans le <code>CPUCreditBalance</code> pour dépasser le niveau de base de l'utilisation de l'UC.</p> <p>Les crédits figurant dans le <code>CPUCreditBalance</code> d'une instance en cours d'exécution n'expirent pas. Lorsqu'une instance T3 ou T3a s'arrête, la valeur <code>CPUCreditBalance</code> est conservée pendant sept jours. Au-delà, tous les crédits accumulés sont perdus. Lorsqu'une instance T2 s'arrête, la valeur de <code>CPUCreditBalance</code> n'est pas conservée, et tous les crédits accumulés sont perdus.</p> <p>Les métriques de crédits CPU sont disponibles toutes les 5 minutes uniquement.</p>		
<code>CPUSurplusCreditBalance</code>	<p>Nombre de crédits excédentaires ayant été dépensés par une instance <code>unlimited</code> lorsque la valeur <code>CPUCreditBalance</code> est nulle.</p> <p>La valeur de <code>CPUSurplusCreditBalance</code> est remboursée progressivement par les crédits UC gagnés. Si le nombre de crédits excédentaires dépasse le nombre maximum de crédits que l'instance peut gagner en 24 heures, les crédits excédentaires dépensés au-dessus du maximum génèrent des frais supplémentaires.</p> <p>Les métriques de crédits CPU sont disponibles toutes les 5 minutes uniquement.</p>	Crédits (minutes vCPU)	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
CPUSurplusCreditsCharged	<p>Nombre de crédits excédentaires dépensés qui ne sont pas remboursés progressivement par les crédits UC gagnés et qui génèrent donc des frais supplémentaires.</p> <p>Les crédits excédentaires dépensés sont facturés lorsque l'une des situations suivantes se produit :</p> <ul style="list-style-type: none"> • Les crédits excédentaires dépensés dépassent le nombre maximum de crédits que l'instance peut gagner sur une période de 24 heures. Les crédits excédentaires dépensés au-dessus de ce maximum sont facturés à la fin de l'heure. • L'instance est arrêtée ou résiliée. • L'instance bascule du mode <code>unlimited</code> au mode <code>standard</code>. <p>Les métriques de crédits CPU sont disponibles toutes les 5 minutes uniquement.</p>	Crédits (minutes vCPU)	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métriques d'hôte dédié

L'espace de noms AWS/EC2 inclut les métriques suivantes pour les hôtes dédiés T3.

Métrique	Description	Unité	Statistiques significatives
DedicatedHostCPUUtilization	Pourcentage de capacité de calcul allouée actuellement utilisée par les instances exécutées sur l'hôte dédié.	Pourcentage	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum

Métrique	Description	Unité	Statistiques significatives
----------	-------------	-------	-----------------------------

- Maximum

Métriques Amazon EBS pour des instances basées sur Nitro

L'espace de noms AWS/EC2 inclut des métriques Amazon EBS supplémentaires pour les volumes attachés aux instances basées sur Nitro qui ne sont pas des instances de type matériel nu.

Métrique	Description	Unité	Statistiques significatives
----------	-------------	-------	-----------------------------

EBSReadOps

Opérations de lecture terminées de tous les volumes Amazon EBS attachés à l'instance au cours de la période spécifiée.

Pour calculer la moyenne d'opérations de lecture d'I/O (IOPS en lecture) pour la période, divisez le nombre total d'opérations de la période par le nombre de secondes de la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour calculer les IOPS en lecture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les opérations par seconde. Par exemple, si vous avez représenté graphiquement `EBSReadOps` CloudWatch comme `m1`, la formule mathématique de la métrique `m1 / (DIFF_TIME(m1))` renvoie la métrique en opérations/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section [Utiliser les mathématiques](#)

Nombre

- Somme
- Moyenne
- Minimum
- Maximum

Métrique	Description	Unité	Statistiques significatives
	métriques dans le guide de CloudWatch l'utilisateur Amazon.		
EBSWriteOps	<p>Opérations d'écriture terminées de tous les volumes EBS attachés à l'instance au cours de la période spécifiée.</p> <p>Pour calculer la moyenne d'opérations d'écriture et d'I/O (IOPS en écriture) pour la période, divisez le nombre total d'opérations de la période par le nombre de secondes de la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour calculer les IOPS en écriture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique DIFF_TIME pour déterminer les opérations par seconde. Par exemple, si vous avez représenté graphiquement EBSWriteOps CloudWatch comme m1, la formule mathématique de la métrique $m1 / (\text{DIFF_TIME}(m1))$ renvoie la métrique en opérations/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques DIFF_TIME et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p>	Nombre	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
EBSReadBytes	<p>Octets lus de tous les volumes EBS attachés à l'instance au cours de la période spécifiée.</p> <p>Le nombre mentionné correspond au nombre d'octets lus pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde en lecture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique <code>DIFF_TIME</code> pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement <code>EBSReadBytes</code> CloudWatch <code>commem1</code>, la formule mathématique de la métrique <code>m1 / (DIFF_TIME(m1))</code> renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques <code>DIFF_TIME</code> et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p>	Octets	<ul style="list-style-type: none">• Somme• Moyenne• Minimum• Maximum

Métrique	Description	Unité	Statistiques significatives
EBSWriteBytes	<p>Octets écrits dans tous les volumes EBS attachés à l'instance au cours de la période spécifiée.</p> <p>Le nombre mentionné correspond au nombre d'octets écrits pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde en écriture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique DIFF_TIME pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement EBSWriteBytes CloudWatch commem1, la formule mathématique de la métrique $m1 / (\text{DIFF_TIME}(m1))$ renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques DIFF_TIME et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p>	Octets	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
EBSIOBalance%	<p>Fournit des informations sur le pourcentage de crédits d'I/O restant dans le compartiment en rafales. Cette métrique est disponible uniquement pour la surveillance basique.</p> <p>Cette métrique n'est disponible que pour certaines tailles d'instance <code>*.4xlarge</code> et plus petites qui atteignent leur performance maximale pendant 30 minutes au moins une fois par 24 heures.</p> <p>La statistique Sum n'est pas applicable pour cette métrique.</p>	Pourcentage	<ul style="list-style-type: none"> • Minimum • Maximum
EBSByteBalance%	<p>Fournit des informations sur le pourcentage de crédits de débit restant dans le compartiment en rafales. Cette métrique est disponible uniquement pour la surveillance basique.</p> <p>Cette métrique n'est disponible que pour certaines tailles d'instance <code>*.4xlarge</code> et plus petites qui atteignent leur performance maximale pendant 30 minutes au moins une fois par 24 heures.</p> <p>La statistique Sum n'est pas applicable pour cette métrique.</p>	Pourcentage	<ul style="list-style-type: none"> • Minimum • Maximum

Pour plus d'informations sur les métriques fournies pour vos volumes EBS, consultez la section [Mesures pour les volumes Amazon EBS dans le guide](#) de l'utilisateur Amazon EBS. Pour plus d'informations sur les métriques fournies pour vos parcs d'instances Spot, consultez [CloudWatch métriques pour Spot Fleet](#).

Métriques de contrôle de statut

Par défaut, les métriques de contrôle de statut sont disponibles à la fréquence d'1 minute sans frais supplémentaires. Pour une instance nouvellement lancée, les données de métriques de contrôle de statut sont disponibles uniquement une fois que l'état d'initialisation de l'instance a pris fin (dans les quelques minutes qui suivent l'entrée de l'instance dans l'état `running`). Pour plus d'informations sur les vérifications de statut EC2, veuillez consulter [Contrôles de statut pour vos instances](#).

L'espace de nom AWS/EC2 inclut les métriques de contrôle de statut suivantes.

Métrique	Description	Unité	Statistiques significatives
StatusCheckFailed	Indique si l'instance a passé avec succès le contrôle de statut d'instance et le contrôle de statut de système au cours de la dernière minute. Cette métrique peut avoir la valeur 0 (succès) ou 1 (échec). Par défaut, cette métrique est disponible à la fréquence d'1 minute sans frais supplémentaires.	Nombre	<ul style="list-style-type: none"> Somme Moyenne
StatusCheckFailed_Instance	Indique si l'instance a passé avec succès le contrôle de statut de l'instance de la dernière minute. Cette métrique peut avoir la valeur 0 (succès) ou 1 (échec). Par défaut, cette métrique est disponible à la fréquence d'1 minute sans frais supplémentaires.	Nombre	<ul style="list-style-type: none"> Somme Moyenne
StatusCheckFailed_System	Indique si l'instance a passé avec succès le contrôle de statut du système de la dernière minute.	Nombre	<ul style="list-style-type: none"> Somme Moyenne

Métrique	Description	Unité	Statistiques significatives
	<p>Cette métrique peut avoir la valeur 0 (succès) ou 1 (échec).</p> <p>Par défaut, cette métrique est disponible à la fréquence d'1 minute sans frais supplémentaires.</p>		
StatusCheckFailed_AttachedEBS	<p>Indique si l'instance a passé avec succès le contrôle de statut de l'EBS attaché de la dernière minute.</p> <p>Cette métrique peut avoir la valeur 0 (succès) ou 1 (échec).</p> <p>Par défaut, cette métrique est disponible à la fréquence d'1 minute sans frais supplémentaires.</p>	Nombre	<ul style="list-style-type: none"> Somme Moyenne

L'AWS/EBS espace de noms inclut la métrique de vérification de statut suivante.

Métrique	Description	Unité	Statistiques significatives
VolumeStalledIOCheck	<p>Remarque : pour les instances Nitro uniquement. Non publié pour les volumes attachés à Amazon ECS et AWS Fargate les tâches.</p> <p>Indique si un volume a réussi ou échoué à une vérification d'E/S bloquée au cours de la dernière minute. Cette métrique peut avoir la valeur 0 (succès) ou 1 (échec).</p>	Nombre	<ul style="list-style-type: none"> Somme Moyenne Minimum Maximum

Métriques de mise en miroir du trafic

L'espace de noms AWS/EC2 inclut des métriques pour le trafic mis en miroir. Pour plus d'informations, consultez [Surveiller le trafic en miroir à l'aide d'Amazon CloudWatch dans le guide Amazon VPC Traffic Mirroring](#).

Métriques du groupe Auto Scaling

L'espace de noms AWS/AutoScaling inclut des métriques pour les groupes Auto Scaling. Pour plus d'informations, consultez la section [Monitor CloudWatch metrics for your Auto Scaling group and instances](#) dans le manuel Amazon EC2 Auto Scaling User Guide.

Dimensions de métriques Amazon EC2

Vous pouvez utiliser les dimensions suivantes pour affiner les métriques répertoriées dans les tableaux précédents.

Dimension	Description
AutoScalingGroupName	Cette dimension filtre les données que vous demandez pour toutes les instances dans un groupe de capacité donné. Un groupe Auto Scaling est un ensemble d'instances que vous définissez si vous utilisez Auto Scaling. Cette dimension est disponible uniquement pour les métriques Amazon EC2 lorsque les instances sont dans un groupe Auto Scaling. Disponible pour les instances avec la surveillance détaillée ou basique activée.
ImageId	Cette dimension filtre les données que vous demandez pour toutes les instances exécutant cette Amazon Machine Image (AMI) Amazon EC2. Disponible pour les instances avec la surveillance détaillée activée.
InstanceId	Cette dimension filtre les données que vous demandez de l'instance identifiée uniquement. Cela vous aide à identifier une instance exacte à partir de laquelle surveiller les données.
InstanceType	Cette dimension filtre les données que vous demandez pour toutes les instances s'exécutant avec ce type d'instance spécifiée. Cela vous permet de classer vos données selon

Dimension	Description
	le type d'instance en cours d'exécution. Par exemple, vous pouvez comparer les données issues d'une instance m1.small et d'une instance m1.large pour déterminer qui a la meilleure valeur commerciale pour votre application. Disponible pour les instances avec la surveillance détaillée activée.

Métriques d'utilisation Amazon EC2

Vous pouvez utiliser les statistiques CloudWatch d'utilisation pour obtenir une visibilité sur l'utilisation des ressources par votre compte. Utilisez ces indicateurs pour visualiser l'utilisation actuelle de vos services sur CloudWatch des graphiques et des tableaux de bord.

Les métriques d'utilisation d'Amazon EC2 correspondent aux quotas de AWS service. Vous pouvez configurer des alarmes qui vous alertent lorsque votre utilisation approche d'un quota de service. Pour plus d'informations sur CloudWatch l'intégration avec les quotas de service, consultez [les statistiques AWS d'utilisation](#) dans le guide de CloudWatch l'utilisateur Amazon.

Amazon EC2 publie les métriques suivantes dans l'espace de noms AWS/Usage.

Métrique	Description
ResourceCount	<p>Nombre des ressources spécifiées exécutées dans votre compte. Les ressources sont définies par les dimensions associées à la métrique.</p> <p>La statistique la plus utile pour cette métrique est MAXIMUM, qui représente le nombre maximal de ressources utilisées pendant la période d'une minute.</p>

Les dimensions suivantes permettent d'affiner les métriques d'utilisation publiées par Amazon EC2.

Dimension	Description
Service	Nom du AWS service contenant la ressource. Pour les métriques d'utilisation d'Amazon EC2, la valeur de cette dimension est EC2.
Type	Type d'entité faisant l'objet d'un rapport. Actuellement, la seule valeur valide pour les métriques d'utilisation d'Amazon EC2 est Resource.
Resource	Type de ressource en cours d'exécution. Actuellement, la seule valeur valide pour les métriques d'utilisation d'Amazon EC2 est vCPU, qui renvoie des informations sur les instances en cours d'exécution.
Class	<p>Classe de ressource suivie. Pour les métriques d'utilisation d'Amazon EC2 avec vCPU comme valeur de la dimension Resource, les valeurs valides sont Standard/OnDemand , F/OnDemand , G/OnDemand , Inf/OnDemand , P/OnDemand et X/OnDemand .</p> <p>Les valeurs de cette dimension définissent la première lettre des types d'instance signalés par la métrique. Par exemple, Standard/OnDemand renvoie des informations sur toutes les instances en cours d'exécution dont les types commencent par A, C, D, H, I, M, R, T et Z, et G/OnDemand renvoie des informations sur toutes les instances en cours d'exécution dont les types commencent par G.</p>

Répertorier les métriques à l'aide de la console

Les métriques sont d'abord regroupées par espace de noms, puis par les différentes combinaisons de dimension au sein de chaque espace de noms. Par exemple, vous pouvez afficher toutes les métriques fournies par Amazon EC2 ou les métriques regroupées par ID d'instance, type d'instance, ID d'image (AMI) ou groupe Auto Scaling.

Pour afficher les métriques disponibles par catégorie (console)

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le volet de navigation, développez Metrics, puis choisissez All metrics.
3. Choisissez l'espace de nom de métrique EC2.

The screenshot shows the AWS CloudWatch console interface. At the top, there are tabs for 'Browse', 'Multi source query', 'Graphed metrics', 'Options', and 'Source'. Below the tabs, there are buttons for 'Add math' and 'Add query'. The main content area is titled 'Metrics (1,153) Info'. There are several interactive elements: a toggle for 'Alarm recommendations', a 'Download alarm code' button, a 'Create alarm' button, 'Graph with SQL' and 'Graph search' buttons, a region selector set to 'Ireland', a search bar with the placeholder 'Search for any metric, dimension, resource id or account id', and a 'Search iGraph' button. The metrics are displayed in a grid of 12 items, each with a category name, a count, and a 'View automatic dashboard' link.

Backup	16	Directory Service	62	EBS	47
EC2	93	EC2/API	152	EC2 Capacity Reservations	8
EC2 Spot	618	EFS	36	Events	1
Logs	3	NATGateway	15	S3	12
SSM Run Command	3	Usage	87		

4. Sélectionnez une dimension de métrique (Per-Instance Metrics (Métriques par instance) par exemple).

The screenshot shows the AWS CloudWatch console interface with the 'Per-Instance Metrics' category selected. The main content area is titled 'Metrics (93) Info'. The search bar now shows 'All > EC2'. The metrics are displayed in a grid of 2 items: 'HostId' with a count of 1 and 'Per-Instance Metrics' with a count of 92.

HostId	1	Per-Instance Metrics	92
--------	---	----------------------	----

5. Pour trier les métriques, utilisez l'en-tête de colonne. Pour représenter graphiquement une métrique, cochez la case en regard de la métrique. Pour filtrer par ressource, sélectionnez l'ID de

ressource, puis Add to search. Pour filtrer par métrique, choisissez le nom de la métrique, puis Add to search (Ajouter à la recherche).

The screenshot shows the AWS CloudWatch console interface. At the top, there are tabs for 'Browse', 'Multi source query', 'Graphed metrics', 'Options', and 'Source'. Below these are buttons for 'Add math' and 'Add query'. The main content area is titled 'Metrics (92) Info' and includes a search bar and several action buttons like 'Download alarm code (14)', 'Create alarm', 'Graph with SQL', and 'Graph search'. A breadcrumb trail shows 'Ireland > All > EC2 > Per-Instance Metrics'. A table lists metrics for various EC2 instances, with columns for 'Instance name', 'Instanceid', 'Metric name', and 'Alarms'. A context menu is open over the 'fingerprint' metric for instance 'i-04747028607e63eaa', showing options: 'Add to search', 'Exclude from search', 'Search for this only', 'Add to graph', 'Graph this metric only', 'Graph all search results', 'Graph with SQL query', 'View In Resource', 'Health', and 'View in EC2 console'.

Listez les métriques à l'aide du AWS CLI

Utilisez la commande [list-metrics](#) pour répertorier les CloudWatch métriques de vos instances.

Pour répertorier toutes les métriques disponibles pour Amazon EC2 (AWS CLI)

L'exemple suivant spécifie l'espace de noms AWS/EC2 pour afficher toutes les métriques pour Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

Voici un exemple de sortie :

```
{
  "Metrics": [
    {
      "Namespace": "AWS/EC2",
      "Dimensions": [
        {
```

```
        "Name": "InstanceId",
        "Value": "i-1234567890abcdef0"
    }
],
"MetricName": "NetworkOut"
},
{
    "Namespace": "AWS/EC2",
    "Dimensions": [
        {
            "Name": "InstanceId",
            "Value": "i-1234567890abcdef0"
        }
    ],
    "MetricName": "CPUUtilization"
},
{
    "Namespace": "AWS/EC2",
    "Dimensions": [
        {
            "Name": "InstanceId",
            "Value": "i-1234567890abcdef0"
        }
    ],
    "MetricName": "NetworkIn"
},
...
]
```

Pour répertorier toutes les métriques disponibles pour une instance (AWS CLI)

L'exemple suivant spécifie l'espace de nom `AWS/EC2` et la dimension `InstanceId` pour afficher les résultats uniquement pour l'instance spécifiée.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --dimensions  
Name=InstanceId,Value=i-1234567890abcdef0
```

Pour répertorier une métrique dans toutes les instances (AWS CLI)

L'exemple suivant spécifie l'espace de nom `AWS/EC2` et un nom de métrique pour afficher les résultats uniquement pour la métrique spécifiée.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --metric-name CPUUtilization
```

Installez et configurez l' CloudWatch agent à l'aide de la console Amazon EC2 pour ajouter des métriques supplémentaires

L'installation et la configuration de l' CloudWatch agent à l'aide de la console Amazon EC2 sont en version bêta pour Amazon EC2 et sont susceptibles d'être modifiées.

Par défaut, Amazon CloudWatch fournit des métriques de base, telles que `CPUUtilization` et `NetworkIn`, pour surveiller vos instances Amazon EC2. Pour collecter des métriques supplémentaires, vous pouvez installer l' CloudWatch agent sur vos instances EC2, puis configurer l'agent pour qu'il émette les métriques sélectionnées. Au lieu d'installer et de configurer manuellement l' CloudWatch agent sur chaque instance EC2, vous pouvez utiliser la console Amazon EC2 pour le faire à votre place.

Cette rubrique explique comment utiliser la console Amazon EC2 pour installer l' CloudWatch agent sur vos instances et configurer l'agent pour qu'il émette des métriques sélectionnées.

Pour les étapes manuelles de ce processus, consultez la section [Installation de l' CloudWatch agent AWS Systems Manager à l'aide](#) du guide de CloudWatch l'utilisateur Amazon. Pour plus d'informations sur l' CloudWatch agent, consultez la section [Collecter les métriques, les journaux et les traces avec l' CloudWatch agent](#).

Rubriques

- [Prérequis](#)
- [Comment ça marche](#)
- [Coûts](#)
- [Installation et configuration de l' CloudWatch agent](#)

Prérequis

Pour utiliser Amazon EC2 afin d'installer et de configurer l' CloudWatch agent, vous devez satisfaire aux exigences relatives à l'utilisateur et à l'instance décrites dans cette section.

Conditions requises pour l'utilisateur

Pour utiliser cette fonctionnalité, l'utilisateur ou le rôle de votre console IAM doit disposer des autorisations requises pour utiliser Amazon EC2 et des autorisations IAM suivantes :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetInstanceProfile",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Conditions préalables à l'instance

- État de l'instance : `running`
- Système d'exploitation pris en charge : Linux
- AWS Systems Manager Agent (agent SSM) : installé. Deux remarques à propos de l'agent SSM :

- L'agent SSM est préinstallé sur certaines Amazon Machine Images (AMI) fournies par des tiers AWS de confiance. Pour plus d'informations sur les AMI prises en charge et les instructions d'installation de l'agent SSM, consultez [Amazon Machine Images \(AMI\) avec l'agent SSM préinstallé](#) dans le guide de l'AWS Systems Manager utilisateur.
- Si vous rencontrez des problèmes avec l'agent SSM, consultez la section [Résolution des problèmes liés à l'agent SSM](#) dans le guide de l'AWS Systems Manager utilisateur.
- Autorisations IAM pour l'instance : les politiques AWS gérées suivantes doivent être ajoutées à un rôle IAM attaché à l'instance :
 - [AmazonSSM ManagedInstance Core](#) — Permet à une instance d'utiliser Systems Manager pour installer et configurer l' CloudWatch agent.
 - [CloudWatchAgentServerPolitique](#) — Permet à une instance d'utiliser l' CloudWatchagent pour y écrire des données CloudWatch.

Pour plus d'informations sur la façon d'ajouter des autorisations IAM à votre instance, consultez la section [Utilisation des profils d'instance](#) dans le guide de l'utilisateur IAM.

Comment ça marche

Avant de pouvoir utiliser la console Amazon EC2 pour installer et configurer l' CloudWatch agent, vous devez vous assurer que votre utilisateur ou rôle IAM, ainsi que les instances sur lesquelles vous souhaitez ajouter des métriques, répondent à certaines conditions préalables. Vous pouvez ensuite utiliser la console Amazon EC2 pour installer et configurer l' CloudWatch agent sur les instances que vous avez sélectionnées.

Répondez d'abord aux [prérequis](#)

- Vous avez besoin des autorisations IAM requises : avant de commencer, assurez-vous que l'utilisateur ou le rôle de votre console dispose des autorisations IAM requises pour utiliser cette fonctionnalité.
- Instances : pour utiliser cette fonctionnalité, vos instances EC2 doivent être des instances Linux, disposer de l'agent SSM installé, disposer des autorisations IAM requises et être en cours d'exécution.

Ensuite, vous pouvez [utiliser la fonctionnalité](#)

1. Sélectionnez vos instances : dans la console Amazon EC2, vous sélectionnez les instances sur lesquelles vous souhaitez installer et configurer l' CloudWatch agent. Vous lancez ensuite le processus en choisissant Configurer CloudWatch l'agent.
2. Valider l'agent SSM : Amazon EC2 vérifie que l'agent SSM est installé et démarré sur chaque instance. Toutes les instances qui échouent à cette vérification sont exclues du processus. L'agent SSM est utilisé pour effectuer des actions sur l'instance au cours de ce processus.
3. Valider les autorisations IAM : Amazon EC2 vérifie que chaque instance dispose des autorisations IAM requises pour ce processus. Toutes les instances qui échouent à cette vérification sont exclues du processus. Les autorisations IAM permettent à l' CloudWatch agent de collecter des métriques à partir de l'instance et de les intégrer AWS Systems Manager pour utiliser l'agent SSM.
4. Valider CloudWatch l'agent : Amazon EC2 vérifie que l' CloudWatch agent est installé et s'exécute sur chaque instance. Si une instance échoue à cette vérification, Amazon EC2 propose d'installer et de démarrer l' CloudWatch agent pour vous. L' CloudWatch agent collectera les métriques sélectionnées sur chaque instance une fois ce processus terminé.
5. Sélectionnez la configuration des métriques : vous sélectionnez les métriques que l' CloudWatch agent doit émettre depuis vos instances. Une fois sélectionné, Amazon EC2 stocke un fichier de configuration dans Parameter Store, où il est conservé jusqu'à la fin du processus. Amazon EC2 supprimera le fichier de configuration de Parameter Store à moins que le processus ne soit interrompu. Notez que si vous ne sélectionnez pas de métrique, mais que vous l'avez déjà ajoutée à votre instance, elle sera supprimée de votre instance une fois ce processus terminé.
6. Mettre à jour la configuration de l' CloudWatch agent : Amazon EC2 envoie la configuration métrique à l' CloudWatch agent. Il s'agit de la dernière étape du processus. En cas de succès, vos instances peuvent émettre des données pour les métriques sélectionnées et Amazon EC2 supprime le fichier de configuration de Parameter Store.

Coûts

Les mesures supplémentaires que vous ajoutez au cours de ce processus sont facturées en tant que mesures personnalisées. Pour plus d'informations sur la tarification des CloudWatch métriques, consultez [Amazon CloudWatch Pricing](#).

Installation et configuration de l' CloudWatch agent

Vous pouvez utiliser la console Amazon EC2 pour installer et configurer l' CloudWatch agent afin d'ajouter des métriques supplémentaires.

Note

Chaque fois que vous effectuez cette procédure, vous remplacez la configuration de l' CloudWatch agent existante. Si vous ne sélectionnez aucune métrique sélectionnée précédemment, elle sera supprimée de l'instance.

Pour installer et configurer l' CloudWatch agent à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez les instances sur lesquelles vous souhaitez installer et configurer l' CloudWatch agent.
4. Choisissez Actions, Surveillance et résolution des problèmes, Configuration de CloudWatch l'agent.

Tip

Cette fonctionnalité n'est pas disponible dans tous les cas Régions AWS. Si CloudWatch l'agent de configuration n'est pas disponible, essayez une autre région.

5. Pour chaque étape du processus, lisez le texte de la console, puis choisissez Next.
6. Pour terminer le processus, dans la dernière étape, sélectionnez Terminer.

Obtenir les statistiques des métriques de vos instances

Vous pouvez obtenir des statistiques relatives aux CloudWatch métriques de vos instances.

Table des matières

- [Vue d'ensemble des statistiques](#)
- [Obtenir les statistiques d'une instance spécifique](#)
- [Regrouper les statistiques à travers les instances](#)
- [Regroupement de statistiques par groupe Auto Scaling](#)
- [Regroupement de statistiques par AMI](#)

Vue d'ensemble des statistiques

Les statistiques sont des agrégations de données métriques sur des périodes spécifiques. CloudWatch fournit des statistiques basées sur les points de données métriques fournis par vos données personnalisées ou fournis par d'autres services AWS connexes CloudWatch. Les regroupements sont effectués en utilisant l'espace de noms, le nom métrique, les dimensions et l'unité de mesure des points de données, pendant la période spécifiée. Le tableau suivant décrit les statistiques disponibles.

Statistique	Description
Minimum	La valeur la plus basse observée pendant la période spécifiée. Vous pouvez utiliser cette valeur pour déterminer les faibles volumes d'activité pour votre application.
Maximum	La valeur la plus haute observée pendant la période spécifiée. Vous pouvez utiliser cette valeur pour déterminer les volumes d'activité élevés pour votre application.
Sum	Toutes les valeurs soumises pour la métrique correspondante ajoutées ensemble. Cette statistique peut être utile pour déterminer le volume total d'une métrique.
Average	La valeur de $\text{Sum} / \text{SampleCount}$ pendant la période spécifiée. En comparant cette statistique à Minimum et à Maximum, vous pouvez déterminer l'ampleur d'une métrique et si l'utilisation moyenne est proche de Minimum ou de Maximum. Cette comparaison vous permet de savoir quand augmenter ou diminuer vos ressources en fonction des besoins.
SampleCount	Le compte (nombre) des points de données utilisé pour le calcul statistique.
pNN.NN	Valeur du centile spécifié. Vous pouvez spécifier un centile en utilisant jusqu'à deux décimales (par exemple, p95.45).

Obtenir les statistiques d'une instance spécifique

Les exemples suivants vous montrent comment utiliser le AWS Management Console ou le AWS CLI pour déterminer l'utilisation maximale du processeur d'une instance EC2 spécifique.

Prérequis

- Vous devez avoir l'ID de l'instance. Vous pouvez obtenir l'ID d'instance en utilisant AWS Management Console ou la commande [describe-instances](#).
- Par défaut, la surveillance basique est activée, mais vous pouvez activer la surveillance détaillée. Pour plus d'informations, consultez [Activer ou désactiver la surveillance détaillée pour vos instances](#).

Pour afficher l'utilisation d'UC d'une instance spécifique (console)

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le volet de navigation, sélectionnez Metrics (Métriques).
3. Choisissez l'espace de nom de métrique EC2.

The screenshot shows the AWS CloudWatch Metrics console interface. At the top, there are tabs for 'Browse', 'Multi source query', 'Graphed metrics', 'Options', and 'Source'. Below the tabs, there are buttons for 'Add math' and 'Add query'. The main content area is titled 'Metrics (1,153) Info' and includes a search bar with the text 'Search for any metric, dimension, resource id or account id'. Below the search bar, there is a grid of metric categories for the 'Ireland' region. Each category is represented by a card with the category name, a count, and a 'View automatic dashboard' link.

Metric Category	Count	View automatic dashboard
Backup	16	View automatic dashboard
Directory Service	62	View automatic dashboard
EBS	47	View automatic dashboard
EC2	93	View automatic dashboard
EC2/API	152	View automatic dashboard
EC2 Capacity Reservations	8	View automatic dashboard
EC2 Spot	618	View automatic dashboard
EFS	36	View automatic dashboard
Events	1	View automatic dashboard
Logs	3	View automatic dashboard
NATGateway	15	View automatic dashboard
S3	12	View automatic dashboard
SSM Run Command	3	View automatic dashboard
Usage	87	View automatic dashboard

4. Choisissez la dimension Per-Instance Metrics (Métriques par instance).

[Browse](#) | [Multi source query](#) | [Graphed metrics](#) | [Options](#) | [Source](#)

[Add math](#) ▼ | [Add query](#) ▼

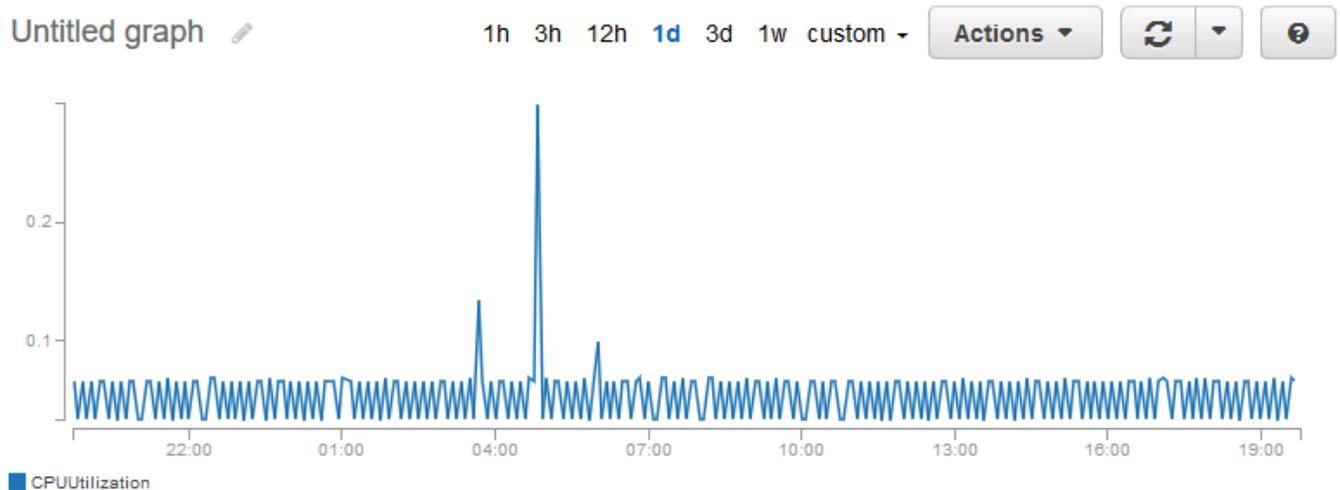
Metrics (93) [Info](#)

Alarm recommendations [Download alarm code \(14\)](#) ▼ | [Create alarm](#) | [Graph with SQL](#) | [Graph search](#)

[Ireland](#) ▼ | [All](#) > [EC2](#) |

HostId	1	Per-Instance Metrics	92
------------------------	---	--------------------------------------	----

5. Dans le champ de recherche, entrez **CPUUtilization**, puis appuyez sur Entrée. Choisissez la ligne de l'instance spécifique, qui contient un graphique pour la métrique CPUUtilization de l'instance. Pour nommer le graphique, choisissez l'icône en forme de crayon. Pour modifier la plage de temps, sélectionnez l'une des valeurs prédéfinies ou choisissez custom.



[All metrics](#) | [Graphed metrics \(1\)](#) | [Graph options](#)

[All](#) > [EC2](#) > [Per-Instance Metrics](#) | [CPUUtilization](#) ✖ |

<input type="checkbox"/>	Instance Name (4) ▲	Instanceid	Metric Name
<input checked="" type="checkbox"/>	my-instance	i-0dcbe8b2653841bd2	CPUUtilization
<input type="checkbox"/>		i-0b6eec80c79f745ad	CPUUtilization

6. Pour modifier la statistique ou la période pour la métrique, choisissez l'onglet Graphed metrics. Sélectionnez l'en-tête de colonne ou une valeur individuelle et choisissez une autre valeur.

All metrics		Graphed metrics (1)		Graph options		
	Label	Namespace	Dimensions	Metric Name	Statistic <input type="checkbox"/>	Period <input type="checkbox"/>
<input checked="" type="checkbox"/>	CPUUtilization	EC2	Dimensions (1)	CPUUtilization	Average	1 Minute 5 Minutes 15 Minutes 1 Hour 6 Hours 1 Day

Pour obtenir l'utilisation d'UC pour une instance spécifique (AWS CLI)

Utilisez la commande suivante [get-metric-statistics](#) afin d'obtenir la métrique CPUUtilization pour l'instance spécifiée à l'aide de la période et de l'intervalle de temps spécifiés :

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
--period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

Voici un exemple de sortie. Chaque valeur représente le pourcentage d'utilisation maximale de l'UC pour une seule instance EC2.

```
{
  "Datapoints": [
    {
      "Timestamp": "2022-10-19T00:18:00Z",
      "Maximum": 0.33000000000000002,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2022-10-19T03:18:00Z",
      "Maximum": 99.670000000000002,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2022-10-19T07:18:00Z",
      "Maximum": 0.34000000000000002,

```

```
    "Unit": "Percent"
  },
  {
    "Timestamp": "2022-10-19T12:18:00Z",
    "Maximum": 0.34000000000000002,
    "Unit": "Percent"
  },
  ...
],
"Label": "CPUUtilization"
}
```

Regrouper les statistiques à travers les instances

Les statistiques agrégées sont disponibles pour des instances pour lesquelles la surveillance détaillée a été activée. Les instances qui utilisent la surveillance basique ne sont pas incluses dans les regroupements. Avant de pouvoir obtenir des statistiques regroupées entre les instances, vous devez [activer la surveillance détaillée](#) (avec coût additionnel) qui fournit des données toutes les minutes.

Notez qu'Amazon CloudWatch ne peut pas agréger les données entre AWS les régions. Les métriques sont totalement séparées d'une région à une autre.

Cet exemple vous montre comment obtenir l'utilisation moyenne de l'UC pour vos instances EC2 à l'aide de la surveillance détaillée. Aucune dimension n'étant spécifiée, CloudWatch renvoie des statistiques pour toutes les dimensions de l'espace de AWS/EC2 noms.

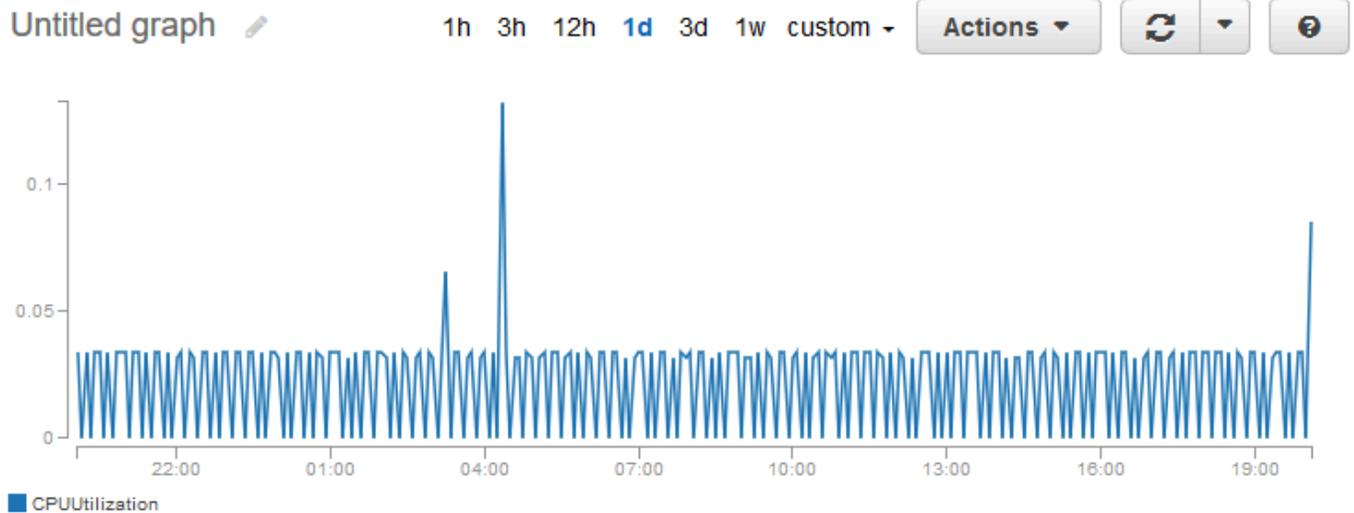
Important

Cette technique de récupération de toutes les dimensions d'un espace de AWS noms ne fonctionne pas pour les espaces de noms personnalisés que vous publiez sur Amazon. CloudWatch Avec les espaces de noms personnalisés, vous devez spécifier l'ensemble complet des dimensions associées à un point de données particulier pour pouvoir extraire les statistiques qui incluent le point de données.

Pour afficher l'utilisation moyenne de l'UC dans vos instances (console)

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le volet de navigation, sélectionnez Metrics (Métriques).

3. Choisissez l'espace de noms EC2, puis choisissez Across All Instances (Sur toutes les instances).
4. Choisissez la ligne contenant CPUUtilization qui affiche un graphique pour la métrique pour toutes vos instances EC2. Pour nommer le graphique, choisissez l'icône en forme de crayon. Pour modifier la plage de temps, sélectionnez l'une des valeurs prédéfinies ou choisissez custom.



5. Pour modifier la statistique ou la période pour la métrique, choisissez l'onglet Graphed metrics. Sélectionnez l'en-tête de colonne ou une valeur individuelle et choisissez une autre valeur.

Pour obtenir l'utilisation moyenne de l'UC sur vos instances (AWS CLI)

Utilisez la commande [get-metric-statistics](#) comme suit pour obtenir l'utilisation moyenne de la métrique CPUUtilization dans vos instances.

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/EC2 \
  --metric-name CPUUtilization \
```

```
--period 3600 --statistics "Average" "SampleCount" \  
--start-time 2022-10-11T23:18:00 \  
--end-time 2022-10-12T23:18:00
```

Voici un exemple de sortie :

```
{  
  "Datapoints": [  
    {  
      "SampleCount": 238.0,  
      "Timestamp": "2022-10-12T07:18:00Z",  
      "Average": 0.038235294117647062,  
      "Unit": "Percent"  
    },  
    {  
      "SampleCount": 240.0,  
      "Timestamp": "2022-10-12T09:18:00Z",  
      "Average": 0.16670833333333332,  
      "Unit": "Percent"  
    },  
    {  
      "SampleCount": 238.0,  
      "Timestamp": "2022-10-11T23:18:00Z",  
      "Average": 0.041596638655462197,  
      "Unit": "Percent"  
    },  
    ...  
  ],  
  "Label": "CPUUtilization"  
}
```

Regroupement de statistiques par groupe Auto Scaling

Vous pouvez regrouper des statistiques pour les instances EC2 dans un groupe Auto Scaling. Notez qu'Amazon CloudWatch ne peut pas agréger les données entre AWS les régions. Les métriques sont totalement séparées d'une région à une autre.

Cet exemple vous montre comment récupérer le nombre total d'octets écrits sur disque pour un groupe Auto Scaling. Le total est calculé par durée d'une minute sur une période de 24 heures pour toutes les instances EC2 dans le groupe Auto Scaling spécifié.

DiskWriteBytes Pour afficher les instances d'un groupe Auto Scaling (console)

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
3. Choisissez l'espace de noms EC2, puis choisissez By Auto Scaling Group (Par groupe Auto Scaling).
4. Choisissez la ligne pour la métrique DiskWriteBytes et le groupe Auto Scaling spécifique, qui affiche un graphique pour la métrique pour les instances du groupe Auto Scaling. Pour nommer le graphique, choisissez l'icône en forme de crayon. Pour modifier la plage de temps, sélectionnez l'une des valeurs prédéfinies ou choisissez custom.
5. Pour modifier la statistique ou la période pour la métrique, choisissez l'onglet Graphed metrics. Sélectionnez l'en-tête de colonne ou une valeur individuelle et choisissez une autre valeur.

DiskWriteBytes Pour afficher les instances d'un groupe Auto Scaling (AWS CLI)

Utilisez la commande [get-metric-statistics](#) comme suit.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
--period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

Voici un exemple de sortie :

```
{
  "Datapoints": [
    {
      "SampleCount": 18.0,
      "Timestamp": "2022-10-19T21:36:00Z",
      "Sum": 0.0,
      "Unit": "Bytes"
    },
    {
      "SampleCount": 5.0,
      "Timestamp": "2022-10-19T21:42:00Z",
      "Sum": 0.0,
      "Unit": "Bytes"
    }
  ],
  "Label": "DiskWriteBytes"
```

}

Regroupement de statistiques par AMI

Vous pouvez regrouper des statistiques pour les instances dont la surveillance détaillée est activée. Les instances qui utilisent la surveillance basique ne sont pas incluses dans les regroupements. Avant de pouvoir obtenir des statistiques regroupées entre les instances, vous devez [activer la surveillance détaillée](#) (avec coût additionnel) qui fournit des données toutes les minutes.

Notez qu'Amazon CloudWatch ne peut pas agréger les données entre AWS les régions. Les métriques sont totalement séparées d'une région à une autre.

Cet exemple vous montre comment déterminer l'utilisation moyenne de l'UC pour toutes les instances qui utilisent une Amazon Machine Image (AMI) spécifique. La moyenne est calculée par intervalles de 60 secondes pour une période d'un jour.

Pour afficher l'utilisation moyenne de l'UC par AMI (console)

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
3. Choisissez l'espace de noms EC2, puis choisissez By Image (AMI) Id (Par ID d'image (AMI)).
4. Choisissez la ligne de la métrique CPUUtilization et l'AMI spécifique, qui affiche un graphique pour la métrique pour l'AMI spécifiée. Pour nommer le graphique, choisissez l'icône en forme de crayon. Pour modifier la plage de temps, sélectionnez l'une des valeurs prédéfinies ou choisissez custom.
5. Pour modifier la statistique ou la période pour la métrique, choisissez l'onglet Graphed metrics. Sélectionnez l'en-tête de colonne ou une valeur individuelle et choisissez une autre valeur.

Pour obtenir l'utilisation moyenne de l'UC pour un ID d'image (AWS CLI)

Utilisez la commande [get-metric-statistics](#) comme suit.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
--period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

Voici un exemple de sortie. Chaque valeur représente le pourcentage d'utilisation moyenne de l'UC pour les instances EC2 exécutant l'AMI spécifiée.

```
{
  "Datapoints": [
    {
      "Timestamp": "2022-10-10T07:00:00Z",
      "Average": 0.041000000000000009,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2022-10-10T14:00:00Z",
      "Average": 0.079579831932773085,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2022-10-10T06:00:00Z",
      "Average": 0.0360000000000000011,
      "Unit": "Percent"
    },
    ...
  ],
  "Label": "CPUUtilization"
}
```

Représenter graphiquement les métriques de vos instances

Après avoir lancé une instance, vous pouvez ouvrir la console Amazon EC2 et afficher les graphiques de surveillance d'une instance dans l'onglet Surveillance. Chaque graphique s'appuie sur l'une des métriques Amazon EC2 disponibles.

Les graphiques suivants sont disponibles :

- Utilisation moyenne de l'UC (pourcentage)
- Lectures moyennes sur disque (octets)
- Ecritures moyennes sur disque (octets)
- Nombre maximal entrées réseau (octets)
- Nombre maximal sorties réseau (octets)
- Récapitulatif des opérations de lecture sur disque (nombre)
- Récapitulatif des opérations d'écriture sur disque (nombre)
- Récapitulatif des statuts (quels qu'il soient)
- Récapitulatif des statuts d'instance (nombre)

- Récapitulatif des statuts système (nombre)

Pour plus d'informations sur les métriques et les données qu'elles leur fournissent, consultez [Répertoriez CloudWatch les métriques disponibles pour vos instances](#).

Représentez graphiquement les métriques à l'aide CloudWatch de

Vous pouvez également utiliser la CloudWatch console pour représenter graphiquement les données métriques générées par Amazon EC2 et d'autres AWS services. Pour plus d'informations, consultez la section [Représentation graphique des métriques](#) dans le guide de CloudWatch l'utilisateur Amazon.

Création d'une CloudWatch alarme pour une instance

Vous pouvez créer une CloudWatch alarme qui surveille les CloudWatch métriques de l'une de vos instances. CloudWatch vous enverra automatiquement une notification lorsque la métrique atteindra le seuil que vous spécifiez. Vous pouvez créer une CloudWatch alarme à l'aide de la console Amazon EC2 ou à l'aide des options plus avancées proposées par la CloudWatch console.

Pour créer une alarme à l'aide de la CloudWatch console

Pour des exemples, consultez la section [Création d' CloudWatch alarmes Amazon](#) dans le guide de CloudWatch l'utilisateur Amazon.

Pour créer une alarme à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.
4. Sur la page détaillée de gestion des CloudWatch alarmes, sous Ajouter ou modifier une alarme, sélectionnez Créer une alarme.
5. Pour Notification d'alarme, choisissez si vous souhaitez configurer les notifications Amazon Simple Notification Service (Amazon SNS). Entrez une rubrique Amazon SNS existante ou entrez un nom pour créer une nouvelle rubrique.
6. Pour Action d'alarme, choisissez si vous souhaitez spécifier une action à effectuer lorsque l'alarme est déclenchée. Choisissez une action dans la liste.

7. Pour Seuils d'alarme, sélectionnez la métrique et les critères de l'alarme. Par exemple, pour créer une alarme qui se déclenche lorsque l'utilisation du processeur atteint 80 % pendant une période de 5 minutes, procédez comme suit :
 - a. Laissez le paramètre par défaut pour Regrouper les exemples par (Moyenne) et Type de données à échantillonner (Utilisation du processeur).
 - b. Choisissez \geq pour Alarme quand et saisissez **0.80** pour Pourcentage.
 - c. Saisissez **1** pour Période consécutive et sélectionnez 5 minutes pour Période.
8. (Facultatif) Pour Exemple de données de métrique, choisissez Ajouter au tableau de bord.
9. Sélectionnez Créer.

Vous pouvez modifier les paramètres de votre CloudWatch alarme depuis la console Amazon EC2 ou depuis la CloudWatch console. Si vous souhaitez supprimer votre alarme, vous pouvez le faire depuis la CloudWatch console. Pour plus d'informations, consultez [Modifier ou supprimer une CloudWatch alarme](#) dans le guide de CloudWatch l'utilisateur Amazon.

Créer des alarmes qui arrêtent, finissent, redémarrent ou récupèrent une instance

À l'aide des actions CloudWatch d'alarme Amazon, vous pouvez créer des alarmes qui arrêtent, mettent fin, redémarrent ou restaurent automatiquement vos instances. Vous pouvez utiliser les actions d'arrêt ou de terminaison pour vous permettre d'économiser de l'argent quand vous n'avez plus besoin qu'une instance s'exécute. De même, les actions de redémarrage et de récupération vous permettent de redémarrer automatiquement ces instances ou de les récupérer sur un nouveau matériel en cas de déficience du nouveau matériel.

Note

Pour les informations de facturation et de tarification d'Amazon CloudWatch Alarmes, consultez la section [CloudWatch facturation et coûts](#) dans le guide de CloudWatch l'utilisateur Amazon.

Le rôle `AWSServiceRoleForCloudWatchEvents` lié au service permet d' AWS effectuer des actions d'alarme en votre nom. La première fois que vous créez une alarme dans l'API AWS Management Console AWS CLI, le ou l'API IAM, le rôle lié au service est CloudWatch créé pour vous.

Il existe un certain nombre de scénarios dans lesquels vous pourriez vouloir arrêter ou terminer automatiquement votre instance. Par exemple, vous pourriez avoir des instances dédiées aux tâches de traitement différé de la paie ou de calcul scientifique qui s'exécutent pendant une durée, puis achèvent leur travail. Plutôt que de laisser ces instances demeurer inactives (et d'accumuler les frais), vous pouvez les arrêter ou les terminer, ce qui peut vous aider à économiser de l'argent. La principale différence entre l'utilisation des actions d'alarme « stop » et « terminate » est que vous pouvez facilement démarrer une instance arrêtée si vous devez l'exécuter à nouveau ultérieurement, et que vous pouvez conserver les mêmes ID d'instance et volume racine. Cependant, vous ne pouvez pas démarrer une instance résiliée. Vous devez à la place lancer une nouvelle instance. Lorsqu'une instance est arrêtée ou résiliée, les données sur les volumes de stockage d'instances sont perdues.

Vous pouvez ajouter les actions d'arrêt, de résiliation, de redémarrage ou de restauration à toute alarme définie sur une métrique Amazon EC2 par instance, y compris les mesures de surveillance de base et détaillées fournies par Amazon CloudWatch (dans l'AWS/EC2 espace de noms), ainsi que toutes les mesures personnalisées incluant la InstanceId dimension, à condition que sa valeur fasse référence à une instance Amazon EC2 en cours d'exécution valide.

Important

Les alarmes de vérification d'état peuvent entrer temporairement dans l'INSUFFICIENT_DATA état s'il manque des points de données métriques. Bien que cela soit rare, cela peut se produire en cas d'interruption des systèmes de reporting des métriques, même lorsqu'une instance est saine. Nous vous recommandons de traiter l'INSUFFICIENT_DATA état comme une donnée manquante plutôt que comme une violation d'alarme, en particulier lorsque vous configurez l'alarme pour arrêter, arrêter, redémarrer ou récupérer une instance.

Prise en charge de la console

Vous pouvez créer des alarmes à l'aide de la console Amazon EC2 ou de la CloudWatch console. Les procédures décrites dans cette documentation utilisent la console Amazon EC2. Pour les procédures utilisant la CloudWatch console, consultez la section [Créer des alarmes qui arrêtent, mettent fin, redémarrent ou restaurent une instance](#) dans le guide de CloudWatch l'utilisateur Amazon.

Autorisations

Vous devez disposer de l'autorisation `iam:CreateServiceLinkedRole` pour créer ou modifier une alarme exécutant des actions d'alarme EC2. Une fonction de service est un [rôle IAM](#) qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.

Table des matières

- [Ajouter des actions d'arrêt aux CloudWatch alarmes Amazon](#)
- [Ajouter des actions de résiliation aux CloudWatch alarmes Amazon](#)
- [Ajouter des actions de redémarrage aux CloudWatch alarmes Amazon](#)
- [Ajouter des actions de restauration aux CloudWatch alarmes Amazon](#)
- [Utilisez la CloudWatch console Amazon pour consulter l'historique des alarmes et des actions](#)
- [Scénarios CloudWatch d'action d'alarme Amazon](#)

Ajouter des actions d'arrêt aux CloudWatch alarmes Amazon

Vous pouvez créer une alarme qui arrête une instance Amazon EC2 quand un certain seuil a été atteint. Par exemple, vous pouvez exécuter des instances de développement ou de test, et, à l'occasion, oublier de les fermer. Vous pouvez créer une alarme qui est déclenchée quand le pourcentage moyen d'utilisation de l'UC a été inférieur à 10 % pendant 24 heures, indiquant que l'instance est inactive et n'est plus en cours d'utilisation. Vous pouvez ajuster le seuil, la durée et la période en fonction de vos besoins ; de plus, vous pouvez ajouter une notification Amazon Simple Notification Service (Amazon SNS) de façon à recevoir un courrier électronique quand l'alarme est déclenchée.

Les instances qui utilisent un volume Amazon EBS comme périphérique racine peuvent être arrêtées ou résiliées, tandis que celles qui recourent au stockage d'instance comme périphérique racine peuvent uniquement être résiliées. Les données stockées sur des volumes de stockage d'instance sont perdues lorsque l'instance est résiliée ou arrêtée.

Pour créer une alarme afin d'arrêter une instance inactive (console Amazon EC2)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.

Vous pouvez également sélectionner le signe plus (



) dans la colonne Alarm status (Statut de l'alarme) .

4. Sur la page Gérer les CloudWatch alarmes, procédez comme suit :
 - a. Sélectionnez Create an alarm (Créer une alarme).
 - b. Pour recevoir un e-mail lorsque l'alarme est déclenchée, sélectionnez une rubrique de Amazon SNS existante pour Alarm notification (Notification d'alarme). Vous devez d'abord créer une rubrique Amazon SNS à l'aide de la console Amazon SNS. Pour plus d'informations, consultez la section [Utilisation d'Amazon SNS pour la messagerie application-to-person \(A2P\) dans le manuel](#) du développeur Amazon Simple Notification Service.
 - c. Activer l'option Alarm action (Action d'alarme), puis sélectionnez Stop (Arrêter).
 - d. Pour Group samples by (Regrouper les échantillons par) et Type of data to sample (Type de données à échantillonner), sélectionnez une statistique et une métrique. Dans cet exemple, sélectionnez Average (Moyenne) et CPU utilization (Utilisation de l'UC).
 - e. Pour Alarm When (Alarme Quand) et Percent (Pourcentage), spécifiez le seuil de la métrique. Dans cet exemple, spécifiez <= et 10 pour cent.
 - f. Pour Consecutive period (Période consécutive) et Period (Période), spécifiez la période d'évaluation de l'alarme. Dans cet exemple, spécifiez 1 période consécutive de 5 Minutes.
 - g. Amazon crée CloudWatch automatiquement un nom d'alarme pour vous. Pour modifier le nom, saisissez un nouveau nom dans Alarm name (Nom de l'alarme). Les noms d'alarme doivent contenir uniquement des caractères ASCII.

 Note

Vous pouvez régler la configuration de l'alarme en fonction de vos propres besoins avant de créer l'alarme, ou pouvez la modifier ultérieurement. Les paramètres de configuration incluent ceux de métrique, de seuil, de durée, d'action et de notification. Cependant, après avoir créé une alarme, vous ne pourrez pas modifier son nom par la suite.

- h. Sélectionnez Créer.

Ajouter des actions de résiliation aux CloudWatch alarmes Amazon

Vous pouvez créer une alarme qui finit automatiquement une instance EC2 quand un certain seuil a été atteint (aussi longtemps que la protection de fin n'est pas activée pour l'instance). Par exemple, il se peut que vous vouliez finir une instance quand elle a terminé son travail et que vous n'avez pas besoin de l'instance à nouveau. Si vous souhaitez utiliser l'instance par la suite, vous devez arrêter l'instance, et non y mettre fin. Les données stockées sur des volumes de stockage d'instance sont perdues lorsque l'instance est résiliée. Pour plus d'informations sur l'activation et la désactivation de la protection contre la résiliation pour une instance, consultez [Activer la protection de la résiliation](#).

Pour créer une alarme afin de résilier une instance inactive (console Amazon EC2)

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.

Vous pouvez également sélectionner le signe plus (



) dans la colonne Alarm status (Statut de l'alarme) .

4. Sur la page Gérer les CloudWatch alarmes, procédez comme suit :
 - a. Sélectionnez Create an alarm (Créer une alarme).
 - b. Pour recevoir un e-mail lorsque l'alarme est déclenchée, sélectionnez une rubrique de Amazon SNS existante pour Alarm notification (Notification d'alarme). Vous devez d'abord créer une rubrique Amazon SNS à l'aide de la console Amazon SNS. Pour plus d'informations, consultez la section [Utilisation d'Amazon SNS pour la messagerie application-to-person \(A2P\) dans le manuel](#) du développeur Amazon Simple Notification Service.
 - c. Activer l'option Alarm action (Action d'alarme), puis sélectionnez Terminate (Résilier).
 - d. Pour Group samples by (Regrouper les échantillons par) et Type of data to sample (Type de données à échantillonner), sélectionnez une statistique et une métrique. Dans cet exemple, sélectionnez Average (Moyenne) et CPU utilization (Utilisation de l'UC).
 - e. Pour Alarm When (Alarme Quand) et Percent (Pourcentage), spécifiez le seuil de la métrique. Dans cet exemple, spécifiez => et 10 pour cent.

- f. Pour Consecutive period (Période consécutive) et Period (Période), spécifiez la période d'évaluation de l'alarme. Dans cet exemple, spécifiez 24 périodes consécutives de 1 heure.
- g. Amazon crée CloudWatch automatiquement un nom d'alarme pour vous. Pour modifier le nom, saisissez un nouveau nom dans Alarm name (Nom de l'alarme). Les noms d'alarme doivent contenir uniquement des caractères ASCII.

 Note

Vous pouvez régler la configuration de l'alarme en fonction de vos propres besoins avant de créer l'alarme, ou pouvez la modifier ultérieurement. Les paramètres de configuration incluent ceux de métrique, de seuil, de durée, d'action et de notification. Cependant, après avoir créé une alarme, vous ne pourrez pas modifier son nom par la suite.

- h. Sélectionnez Créer.

Ajouter des actions de redémarrage aux CloudWatch alarmes Amazon

Vous pouvez créer une CloudWatch alarme Amazon qui surveille une instance Amazon EC2 et redémarre automatiquement l'instance. L'action d'alarme de redémarrage est recommandée pour les défaillances de vérification de l'état d'instance (par opposition à l'action d'alarme de récupération, qui convient aux défaillances de la vérification de l'état du système). Le redémarrage d'une instance est similaire à celui d'un système d'exploitation. Dans la plupart des cas, il suffit de quelques minutes pour redémarrer votre instance. Lorsque vous redémarrez une instance, elle reste sur le même hôte physique, ce qui signifie qu'elle conserve son nom DNS public, son adresse IP privée et toutes les données se trouvant sur ses volumes de stockage d'instance.

Le redémarrage d'une instance ne déclenche pas de nouvelle période de facturation d'instance (avec frais d'une minute minimum), contrairement à l'arrêt, puis au redémarrage d'une instance. Les données des volumes de stockage d'instances sont conservées lorsque l'instance est redémarrée. Les volumes de stockage d'instances doivent être remontés dans le système de fichiers après un redémarrage. Pour plus d'informations, consultez [Redémarrer votre instance](#).

 Important

Pour prévenir toute condition de concurrence entre les actions de redémarrage et de récupération, évitez de définir le même nombre de périodes d'évaluation pour une alarme

de redémarrage et une alarme de récupération. Nous vous recommandons de définir des alarmes de redémarrage sur trois périodes d'évaluation d'une minute chacune. Pour plus d'informations, consultez la section [Évaluation d'une alarme](#) dans le guide de CloudWatch l'utilisateur Amazon.

Pour créer une alarme afin de redémarrer une instance (console Amazon EC2)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.

Vous pouvez également sélectionner le signe plus (



) dans la colonne Alarm status (Statut de l'alarme) .

4. Sur la page Gérer les CloudWatch alarmes, procédez comme suit :
 - a. Sélectionnez Create an alarm (Créer une alarme).
 - b. Pour recevoir un e-mail lorsque l'alarme est déclenchée, sélectionnez une rubrique de Amazon SNS existante pour Alarm notification (Notification d'alarme). Vous devez d'abord créer une rubrique Amazon SNS à l'aide de la console Amazon SNS. Pour plus d'informations, consultez la section [Utilisation d'Amazon SNS pour la messagerie application-to-person \(A2P\) dans le manuel](#) du développeur Amazon Simple Notification Service.
 - c. Activer l'option Alarm action (Action d'alarme), puis sélectionnez Reboot (Redémarrer).
 - d. Pour Group samples by (Regrouper les échantillons par) et Type of data to sample (Type de données à échantillonner), sélectionnez une statistique et une métrique. Dans cet exemple, sélectionnez Average (Moyenne) et Status check failed: instance (Échec du contrôle de statut : instance).
 - e. Pour Consecutive period (Période consécutive) et Period (Période), spécifiez la période d'évaluation de l'alarme. Pour cet exemple, entrez 3 périodes consécutives de 5 minutes.
 - f. Amazon crée CloudWatch automatiquement un nom d'alarme pour vous. Pour modifier le nom, saisissez un nouveau nom dans Alarm name (Nom de l'alarme). Les noms d'alarme doivent contenir uniquement des caractères ASCII.

g. Sélectionnez Créer.

Ajouter des actions de restauration aux CloudWatch alarmes Amazon

Vous pouvez créer une CloudWatch alarme Amazon qui surveille une instance Amazon EC2. Si l'instance est altérée en raison d'une défaillance matérielle sous-jacente ou d'un problème nécessitant une AWS intervention pour être réparée, vous pouvez la récupérer automatiquement. Les instances mises hors service ne peuvent pas être récupérées. Une instance récupérée est identique à l'instance d'origine, y compris pour l'ID d'instance, les adresses IP privées, les adresses IP Elastic et toutes les métadonnées de l'instance.

CloudWatch vous empêche d'ajouter une action de restauration à une alarme qui se trouve sur une instance qui ne prend pas en charge les actions de restauration.

Lorsque l'alarme `StatusCheckFailed_System` est déclenchée et que l'action de récupération est initiée, vous en êtes averti par la rubrique Amazon SNS que vous avez choisie quand vous avez créé l'alarme et associé l'action de récupération. Lors de la récupération d'instance, l'instance est migrée pendant un redémarrage d'instance, et toutes les données en mémoire sont perdues. Lorsque le processus est terminé, les informations sont publiées dans la rubrique SNS que vous avez configurée pour l'alarme. Toutes les personnes abonnées à cette rubrique SNS reçoivent une notification par e-mail qui inclut le statut de la tentative de récupération et les éventuelles instructions supplémentaires. Vous remarquez un redémarrage d'instance sur l'instance récupérée.

 Note

L'action de récupération ne peut être utilisée qu'avec `StatusCheckFailed_System`, pas avec `StatusCheckFailed_Instance`.

Les problèmes suivants peuvent entraîner l'échec des contrôles de statut de système :

- Perte de connectivité réseau
- Perte d'alimentation système
- Problèmes logiciels sur un hôte physique
- Problèmes matériels sur un hôte physique ayant un impact sur l'accessibilité du réseau

L'opération de récupération est prise en charge uniquement sur les instances présentant certaines caractéristiques. Pour plus d'informations, consultez [Résilience de l'instance](#).

Si votre instance a une adresse IP publique, elle la conserve après la récupération.

 Important

Pour prévenir toute condition de concurrence entre les actions de redémarrage et de récupération, évitez de définir le même nombre de périodes d'évaluation pour une alarme de redémarrage et une alarme de récupération. Nous vous recommandons de définir des alarmes de récupération sur deux périodes d'évaluation d'une minute chacune. Pour plus d'informations, consultez la section [Évaluation d'une alarme](#) dans le guide de CloudWatch l'utilisateur Amazon.

Pour créer une alarme afin de récupérer une instance (console Amazon EC2)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Actions, Surveiller et dépanner, Gérer les CloudWatch alarmes.

Vous pouvez également sélectionner le signe plus (



) dans la colonne Alarm status (Statut de l'alarme) .

4. Sur la page Gérer les CloudWatch alarmes, procédez comme suit :
 - a. Sélectionnez Create an alarm (Créer une alarme).
 - b. Pour recevoir un e-mail lorsque l'alarme est déclenchée, sélectionnez une rubrique de Amazon SNS existante pour Alarm notification (Notification d'alarme). Vous devez d'abord créer une rubrique Amazon SNS à l'aide de la console Amazon SNS. Pour plus d'informations, consultez la section [Utilisation d'Amazon SNS pour la messagerie application-to-person \(A2P\) dans le manuel](#) du développeur Amazon Simple Notification Service.

Note

Les utilisateurs doivent s'abonner à la rubrique SNS spécifiée pour recevoir des notifications par e-mail lorsque l'alarme se déclenche. Il reçoit Utilisateur racine d'un compte AWS toujours des notifications par e-mail lorsque des actions de restauration automatique d'instance se produisent, même si aucune rubrique SNS n'est spécifiée ou si l'utilisateur root n'est pas abonné à la rubrique SNS spécifiée.

- c. Activer l'option Alarm action (Action d'alarme), puis sélectionnez Recover (Récupérer).
- d. Pour Group samples by (Regrouper les échantillons par) et Type of data to sample (Type de données à échantillonner), sélectionnez une statistique et une métrique. Dans cet exemple, sélectionnez Average (Moyenne) et Status check failed: system (Échec du contrôle de statut : système).
- e. Pour Consecutive period (Période consécutive) et Period (Période), spécifiez la période d'évaluation de l'alarme. Pour cet exemple, entrez 2 périodes consécutives de 5 minutes.
- f. Amazon crée CloudWatch automatiquement un nom d'alarme pour vous. Pour modifier le nom, saisissez un nouveau nom dans Alarm name (Nom de l'alarme). Les noms d'alarme doivent contenir uniquement des caractères ASCII.
- g. Sélectionnez Créer.

Utilisez la CloudWatch console Amazon pour consulter l'historique des alarmes et des actions

Vous pouvez consulter l'historique des alarmes et des actions dans la CloudWatch console Amazon. Amazon CloudWatch conserve l'historique des alarmes et des actions des deux dernières semaines.

Pour consulter l'historique des alarmes et des actions déclenchées (CloudWatch console)

1. Ouvrez la CloudWatch console à l'[adresse https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le panneau de navigation, cliquez sur Alarms.
3. Sélectionnez une alarme.
4. L'onglet Détails affiche la transition d'état la plus récente, ainsi que les valeurs de date et de métrique.
5. Choisissez l'onglet Historique pour afficher les entrées les plus récentes de l'historique.

Scénarios CloudWatch d'action d'alarme Amazon

Vous pouvez utiliser la console Amazon EC2 pour créer des actions d'alarme qui arrêtent ou finissent une instance Amazon EC2 quand certaines conditions sont satisfaites. Dans la capture d'écran suivante de la page de la console où vous avez défini les actions d'alarme, nous avons numéroté les paramètres. Nous avons également numéroté les paramètres des scénarios qui suivent afin de vous aider à créer les actions appropriées.

New console

The screenshot shows the configuration interface for an Amazon CloudWatch alarm. It is divided into three main sections: Alarm notification, Alarm action, and Alarm thresholds. Each section has a title, a brief description, and a toggle switch. The Alarm notification section includes a search input field. The Alarm action section includes a dropdown menu. The Alarm thresholds section includes several input fields and dropdown menus for configuring the alarm's logic. A red bracket on the left side of the Alarm action section highlights the dropdown menu, and a red circle with the number '1' is placed next to it. Other numbered callouts (2-7) are placed on various input fields throughout the form.

Alarm notification [Info](#)

Configure the alarm to send notifications to an Amazon SNS topic when it is triggered.

1

Alarm action [Info](#)

Specify the action to take when the alarm is triggered.

Alarm thresholds

Specify the metric thresholds for the alarm.

Group samples by age

Type of data to sample

Alarm When

Consecutive Period Period nutes

Alarm name

Old console

Create Alarm ✕

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.
To edit an alarm, first choose whom to notify and then define when the notification should be sent.

1 **Send a notification to:** [create topic](#)

Take the action:

- Recover this instance (i)
- Stop this instance (i)
- Terminate this instance (i)
- Reboot this instance (i)

Whenever: **2** of **3**

Is: **4** **5** Percent

For at least: **6** consecutive period(s) of **7**

Name of alarm:

Cancel
Create Alarm

CPU Utilization Percent

Scénario 1 : arrêter le développement inactif et tester les instances

Créez une alarme qui arrête une instance utilisée pour le développement ou le test de logiciels quand elle a été inactive pendant au moins une heure.

Paramètre	Value
1	Arrêter
2	Maximum
3	CPU Utilization
4	<=
5	10 %
6	1
7	1 heure

Scénario 2 : arrêter les instances inactives

Créez une alarme qui arrête une instance et envoie un courrier électronique quand l'instance est inactive depuis 24 heures.

Paramètre	Value
1	Arrêter et envoyer un e-mail
2	Moyenne
3	CPU Utilization
4	<=
5	5 %
6	24
7	1 heure

Scénario 3 : envoyer un e-mail relatif aux serveurs Web ayant un trafic inhabituellement élevé

Créez une alarme qui envoie un courrier électronique quand une instance dépasse 10 Go de trafic réseau sortant par jour.

Paramètre	Value
1	E-mail
2	Somme
3	Réseau sortant
4	>
5	10 Go
6	24

Paramètre	Value
7	1 heure

Scénario 4 : arrêter les serveurs Web avec un trafic inhabituellement élevé

Créez un alarme qui arrête une instance et envoie un SMS quand le trafic sortant excède 1 Go par heure.

Paramètre	Value
1	Arrêter et envoyer un SMS
2	Somme
3	Réseau sortant
4	>
5	1 Go
6	1
7	1 heure

Scénario 5 : arrêter une instance déficiente

Créez une alarme qui arrête une instance après qu'elle a échoué à trois contrôles de statut consécutifs (exécutés à 5 minutes d'intervalle).

Paramètre	Value
1	Arrêter
2	Moyenne
3	Échec du contrôle de du statut : Système
4	-

Paramètre	Value
5	-
6	1
7	15 minutes

Scénario 6 : résilier les instances quand les tâches de traitement par batch sont terminés

Créez une alarme qui finit une instance exécutant des traitements par batch quand elle n'envoie plus de données de résultat.

Paramètre	Value
1	Terminer
2	Maximum
3	Réseau sortant
4	<=
5	100,000 bytes
6	1
7	5 minutes

Automatisez Amazon EC2 en utilisant EventBridge

Vous pouvez utiliser Amazon EventBridge pour automatiser Services AWS et répondre automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez créer des règles pour indiquer quels événements vous intéressent et les actions à effectuer quand un événement correspond à une règle. Les actions pouvant être déclenchées automatiquement sont les suivantes :

- Invoquer une AWS Lambda fonction
- Appeler Run Command (Exécuter la commande) d'Amazon EC2
- Relayer l'événement à Amazon Kinesis Data Streams
- Activer une machine à AWS Step Functions états
- Notifier une rubrique Amazon SNS
- Notifier une file d'attente Amazon SQS

Voici des exemples de la manière dont vous pouvez utiliser EventBridge Amazon EC2 :

- Activer une fonction Lambda chaque fois qu'une instance entre dans l'état d'exécution.
- Notifier une rubrique Amazon SNS lorsqu'un volume Amazon EBS est créé ou modifié.
- Envoyez une commande à une ou plusieurs instances Amazon EC2 à l'aide d'Amazon EC2 Run Command chaque fois qu'un certain événement se produit dans AWS un autre service.

Pour plus d'informations, consultez le [guide de EventBridge l'utilisateur Amazon](#).

Types d'événements Amazon EC2

Amazon EC2 prend en charge les types d'événements suivants :

- [Changement d'état de l'AMI EC2](#)
- [Notification de changement d'état de lancement rapide EC2](#)
- [Erreur de flotte EC2](#)
- [Informations sur la flotte EC2](#)
- [Modification de l'instance de flotte EC2](#)
- [Modification de la demande d'instance Spot de flotte EC2](#)
- [Changement d'état du flotte EC2](#)
- [Recommandation de rééquilibrage des instances EC2](#)
- [Notification de changement d'état de l'instance EC2](#)
- [Erreur de parc d'instances Spot EC2](#)
- [Informations sur le parc d'instances Spot EC2](#)
- [Modification de l'instance de parc d'instances Spot EC2](#)
- [Modification de la demande d'instance Spot de parc d'instances Spot EC2](#)

- [Changement d'état du parc d'instances Spot EC2](#)
- [Avertissement d'interruption d'une instance Spot EC2](#)
- [Exécution de demande d'instance Spot EC2](#)
- [Notification de sous-utilisation des réserves de capacité à la demande \(OCDR\) EC2](#)

Pour plus d'informations sur les types d'événements pris en charge par Amazon EBS, consultez [EventBridge Amazon EBS](#).

Enregistrez les appels d'API Amazon EC2 à l'aide de AWS CloudTrail

L'API Amazon EC2 est intégrée à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un. Service AWS CloudTrail capture tous les appels d'API pour Amazon EC2 sous forme d'événements, y compris les appels depuis la console et les appels de code vers les opérations d'API. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à l'API Amazon EC2, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite, etc.

Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Informations sur l'API Amazon EC2 dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Amazon EC2 et Amazon EBS, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#).

Pour obtenir un registre continu des événements dans votre Compte AWS, y compris les événements pour Amazon EC2 et Amazon EBS, créez un journal d'activité. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez :

- [Création d'un parcours pour votre Compte AWS](#)
- [Service AWS intégrations avec des journaux CloudTrail](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Toutes les actions Amazon EC2 et les actions de gestion Amazon EBS sont enregistrées CloudTrail et documentées dans le manuel [Amazon EC2 API Reference](#). Par exemple, les appels au [RunInstancesDescribeInstances](#), ou [CreateImage](#) les actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur IAM.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

Pour plus d'informations, consultez l'[CloudTrail user identity élément](#).

Comprendre les entrées du fichier journal de l'API Amazon EC2

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'enregistrement de fichier journal suivant montre qu'un utilisateur a résilié une instance.

```
{
  "Records": [
    {
```

```
"eventVersion":"1.03",
"userIdentity":{
  "type":"Root",
  "principalId":"123456789012",
  "arn":"arn:aws:iam::123456789012:root",
  "accountId":"123456789012",
  "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
  "userName":"user"
},
"eventTime":"2016-05-20T08:27:45Z",
"eventSource":"ec2.amazonaws.com",
"eventName":"TerminateInstances",
"awsRegion":"us-west-2",
"sourceIPAddress":"198.51.100.1",
"userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
"requestParameters":{
  "instancesSet":{
    "items":[{
      "instanceId":"i-1a2b3c4d"
    }]
  }
},
"responseElements":{
  "instancesSet":{
    "items":[{
      "instanceId":"i-1a2b3c4d",
      "currentState":{
        "code":32,
        "name":"shutting-down"
      },
      "previousState":{
        "code":16,
        "name":"running"
      }
    }]
  }
},
"requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
"eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
"eventType":"AwsApiCall",
"recipientAccountId":"123456789012"
}
]
```

```
}
```

AWS CloudTrail À utiliser pour auditer les connexions établies à l'aide d'EC2 Instance Connect

AWS CloudTrail À utiliser pour auditer les utilisateurs qui se connectent à vos instances via EC2 Instance Connect.

Pour auditer l'activité SSH via EC2 Instance Connect à l'aide de la console AWS CloudTrail

1. Ouvrez la CloudTrail console à l'[adresse https://console.aws.amazon.com/cloudtrail/](https://console.aws.amazon.com/cloudtrail/).
2. Vérifiez que vous êtes dans la région correcte.
3. Dans le volet de navigation, sélectionnez Event history (Historique des événements).
4. Pour Filter (Filtre), choisissez Event source (Source de l'événement), `ec2-instance-connect.amazonaws.com`.
5. (Facultatif) Pour Time range (Plage de temps), sélectionnez une plage de temps.
6. Choisissez l'icône Refresh events (Actualiser les événements).
7. La page affiche les événements correspondant aux appels d'API [SendSSHPublicKey](#). Développez un événement à l'aide de la flèche pour afficher des détails supplémentaires, tels que le nom d'utilisateur et la clé d'AWS accès utilisés pour établir la connexion SSH, ainsi que l'adresse IP source.
8. Pour afficher toutes les informations sur l'événement au format JSON, choisissez Afficher l'événement. Le champ `requestParameters` contient l'ID de l'instance de destination, le nom d'utilisateur OS et la clé publique qui ont été utilisés pour établir la connexion SSH.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "ABCDEFGONGNOM00CB6XYTQEXAMPLE",
    "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
    "accountId": "123456789012",
    "accessKeyId": "ABCDEFGUKZHNAW40SN2AEXAMPLE",
    "userName": "IAM-friendly-name",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-09-21T21:37:58Z"}
    }
  }
}
```

```
    }
  },
  "eventTime": "2018-09-21T21:38:00Z",
  "eventSource": "ec2-instance-connect.amazonaws.com",
  "eventName": "SendSSHPublicKey ",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.456.789.012",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": {
    "instanceId": "i-0123456789EXAMPLE",
    "osUser": "ec2-user",
    "SSHKey": {
      "publicKey": "ssh-rsa ABCDEFGHIJKLMNOP01234567890EXAMPLE"
    }
  },
  "responseElements": null,
  "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
  "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
  "eventType": "AwsApiCall",
  "recipientAccountId": "0987654321"
}
```

Si vous avez configuré votre AWS compte pour collecter des CloudTrail événements dans un compartiment S3, vous pouvez télécharger et auditer les informations par programmation. Pour plus d'informations, consultez la section [Obtenir et consulter vos fichiers CloudTrail journaux](#) dans le guide de AWS CloudTrail l'utilisateur.

Surveillez vos applications .NET et SQL Server avec CloudWatch Application Insights

CloudWatch Application Insights vous aide à surveiller vos applications .NET et SQL Server qui utilisent des instances Amazon EC2 ainsi que d'autres ressources [AWS applicatives](#). Cette solution identifie et configure des journaux de métriques clés et des alarmes sur vos ressources d'application et votre pile technologique (par exemple, votre base de données Microsoft SQL Server, les serveurs Web (IIS) et d'applications, le système d'exploitation, les équilibreurs de charge et les files d'attente). Elle surveille en permanence les métriques et les journaux afin de détecter et de corrélérer les anomalies et les erreurs. Lorsque des erreurs et des anomalies sont détectées, Application Insights génère [CloudWatch des événements](#) que vous pouvez utiliser pour configurer des notifications ou prendre des mesures. Pour faciliter le dépannage, elle crée des tableaux de bord automatisés qui

retracent les problèmes détectés, les anomalies métriques, les erreurs de journalisation corrélées, ainsi que des informations supplémentaires vous indiquant la cause potentielle. Les tableaux de bord automatisés vous aident à prendre rapidement des mesures correctives pour vous assurer que vos applications sont saines et que les utilisateurs finaux ne sont pas affectés.

Pour consulter la liste complète des journaux et mesures pris en charge, consultez la section [Journaux et mesures pris en charge par Amazon CloudWatch Application Insights](#).

Informations fournies sur les problèmes détectés

- Un bref résumé du problème
- La date et l'heure de début du problème
- La gravité du problème : High/Medium/Low (Haute/Moyenne/Basse)
- Le statut du problème détecté : In-progress/Resolved (En cours/Résolu)
- Analyses : génération automatique d'analyses concernant le problème détecté et sa possible cause
- Commentaires sur les informations : commentaires que vous avez fournis sur l'utilité des informations générées par CloudWatch Application Insights pour .NET et SQL Server
- Observations connexes : une vue détaillée des anomalies métriques et des extraits pertinents de journaux d'erreurs liés au problème, parmi différents composants d'application

Commentaires

Vous pouvez fournir des commentaires sur les analyses générées automatiquement relatives aux problèmes détectés en les qualifiant d'utiles ou d'inutiles. Les commentaires que vous laissez sur les analyses, ainsi que vos diagnostics d'application (anomalies métriques et exceptions de journaux) sont utilisés pour améliorer les futures détections de problèmes similaires.

Pour plus d'informations, consultez la documentation [CloudWatchApplication Insights](#) dans le guide de CloudWatch l'utilisateur Amazon.

Suivez votre utilisation du niveau gratuit pour Amazon EC2

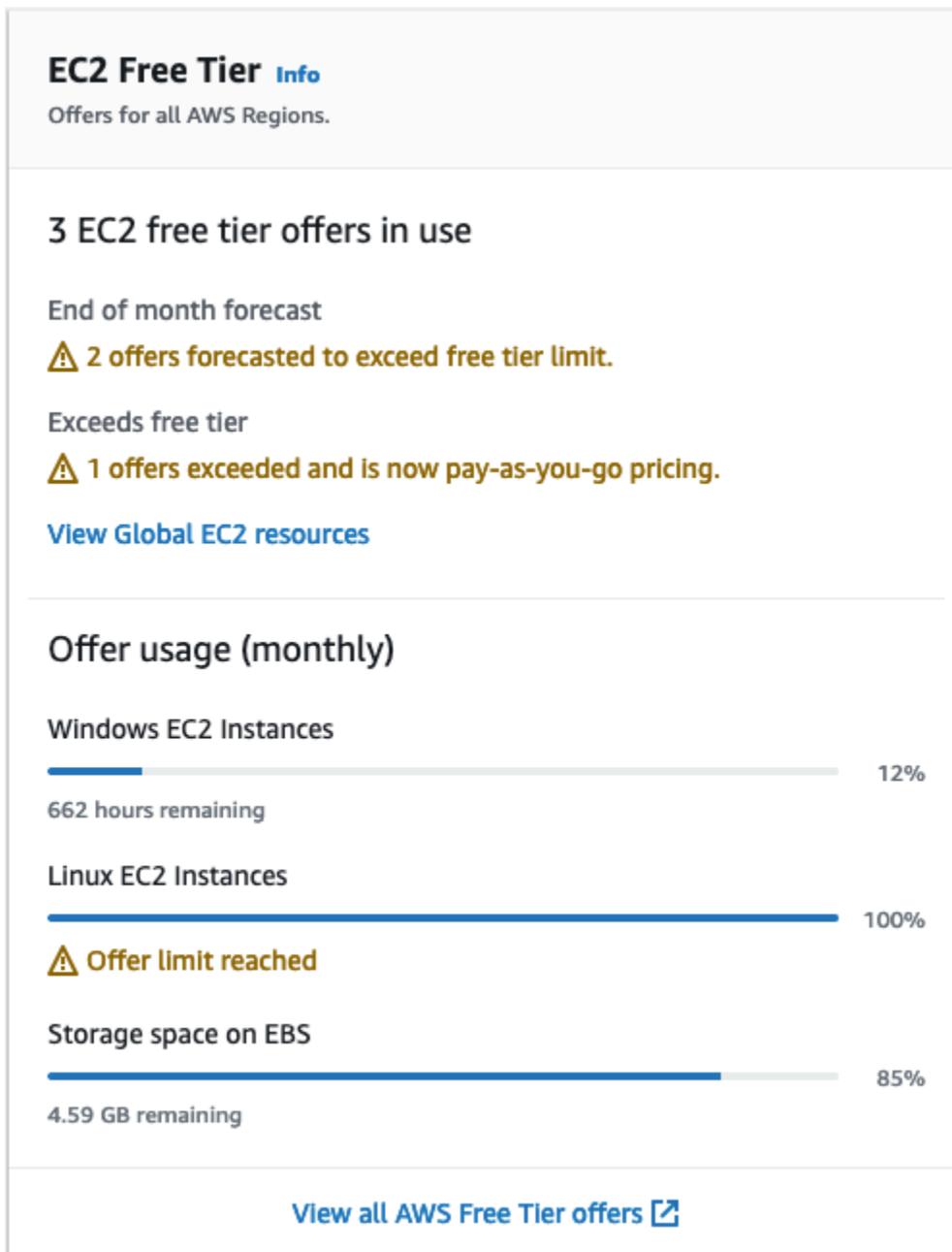
Vous pouvez utiliser Amazon EC2 sans frais si vous êtes AWS client depuis moins de 12 mois et si vous respectez les limites d'utilisation. Niveau gratuit d'AWS Il est important de suivre votre utilisation de l'offre gratuite pour éviter les surprises liées à la facturation. Si vous dépassez les limites du niveau gratuit, vous devrez payer des pay-as-go frais standard.

 Note

Si vous êtes AWS client depuis plus de 12 mois, vous n'êtes plus éligible à l'utilisation du niveau gratuit et vous ne verrez pas la case du niveau gratuit EC2 décrite dans la procédure suivante.

Pour suivre votre utilisation de l'offre gratuite

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Tableau de bord du EC2.
3. Recherchez la case Offre gratuite EC2 (en haut à droite).



4. Dans la case Offre gratuite EC2, vérifiez votre utilisation de l'offre gratuite, comme suit :
- Sous Offres gratuites EC2 en cours d'utilisation, prenez note des avertissements :
 - Prévisions de fin de mois : vous avertit que des frais vous seront facturés ce mois si vous continuez avec votre modèle d'utilisation actuel.
 - Dépasse l'offre gratuite : indique que vous avez dépassé les limites de l'offre gratuite et que vous avez déjà engagé des frais.

- Sous Utilisation de l'offre (mensuelle), notez votre utilisation des instances Linux, des instances Windows et du stockage EBS. Le pourcentage indique la part des limites de l'offre gratuite que vous avez utilisée ce mois-ci. Si vous êtes à 100 %, des frais vous seront facturés pour toute utilisation ultérieure.

 Note

Ces informations apparaissent uniquement une fois que vous avez créé une instance. Toutefois, les informations relatives à l'utilisation ne sont pas mises à jour en temps réel, mais trois fois par jour.

5. Pour éviter d'encourir des frais supplémentaires, supprimez toutes les ressources qui sont actuellement facturées ou qui le seront si vous dépassez la limite d'utilisation de votre offre gratuite.
 - Pour obtenir les instructions relatives à la suppression de votre instance, passez à l'étape suivante de ce didacticiel.
 - Pour vérifier si vous disposez de ressources dans d'autres régions qui sont susceptibles d'être facturées, dans la case Offre gratuite EC2, choisissez Afficher les ressources EC2 globales et ouvrir la vue globale EC2. Pour plus d'informations, consultez [Amazon EC2 Global View \(Amazon EC2 Global View\)](#).
6. Pour afficher l'utilisation de vos ressources pour Services AWS tous Niveau gratuit d'AWS, en bas de la case EC2 Free Tier, choisissez Afficher toutes les Niveau gratuit d'AWS offres. Pour plus d'informations, consultez [Utilisation de la Niveau gratuit d'AWS](#) dans le Guide de l'utilisateur de la facturation AWS .

Mise en réseau dans Amazon EC2

Amazon VPC vous permet de lancer AWS des ressources, telles que des instances Amazon EC2, dans un réseau virtuel dédié à AWS votre compte, connu sous le nom de cloud privé virtuel (VPC). Lorsque vous lancez une instance, vous pouvez sélectionner un sous-réseau à partir du VPC. L'instance est configurée avec une interface réseau principale, qui est une carte réseau virtuelle logique. L'instance reçoit une adresse IP privée principale de l'adresse IPv4 du sous-réseau et elle est affectée à l'interface réseau principale.

Vous pouvez contrôler si l'instance reçoit une adresse IP publique du pool d'adresses IP publiques d'Amazon. L'adresse IP publique d'une instance est associée à votre instance uniquement jusqu'à ce qu'elle soit arrêtée ou résiliée. Si vous avez besoin d'une adresse IP publique persistante, vous pouvez attribuer une adresse IP élastique à votre AWS compte et l'associer à une instance ou à une interface réseau. Une adresse IP élastique reste associée à votre AWS compte jusqu'à ce que vous la publiiez, et vous pouvez la déplacer d'une instance à l'autre selon vos besoins. Vous pouvez apporter votre propre plage d'adresses IP à votre compte AWS, où elle apparaît sous la forme d'un pool d'adresses, puis allouer des adresses IP Elastic à partir de votre pool d'adresses.

Pour augmenter les performances réseau et réduire la latence, vous pouvez lancer des instances dans un groupe de placement. Vous pouvez obtenir des performances de paquets par seconde (PPS) nettement plus élevées grâce à la mise en réseau améliorée. Vous pouvez accélérer les applications de calcul hautes performances et de Machine Learning à l'aide d'un Elastic Fabric Adapter (EFA), qui est un appareil réseau que vous pouvez attacher à un type d'instance pris en charge.

Fonctions

- [Régions et zones](#)
- [Adressage IP des instances Amazon EC2](#)
- [Types de noms d'hôtes des instances Amazon EC2](#)
- [Fourniture de vos propres adresses IP \(BYOIP\) dans Amazon EC2](#)
- [Adresses IP Elastic](#)
- [Interfaces réseau Elastic](#)
- [Bande passante réseau d'instance Amazon EC2](#)
- [Mise en réseau améliorée sur Amazon EC2](#)
- [Elastic Fabric Adapter](#)

- [Topologie d'instance Amazon EC2](#)
- [Groupes de placement](#)
- [Unité de transmission maximale \(MTU\) du réseau pour votre instance EC2](#)
- [Clouds privés virtuels pour vos instances EC2](#)

Régions et zones

Amazon EC2 est hébergé à plusieurs endroits dans le monde. Ces emplacements sont composés de zones de disponibilité Régions AWS, de zones locales et de zones de longueur d'onde. AWS Outposts

- Chaque région constitue une zone géographique séparée.
- Les zones de disponibilité sont des emplacements multiples isolés dans chaque région.
- Les Local Zones vous permettent de placer des ressources, telles que le calcul et le stockage, dans plusieurs emplacements plus proches de vos utilisateurs finaux.
- AWS Outposts apporte AWS des services, une infrastructure et des modèles d'exploitation natifs à pratiquement tous les centres de données, espaces de colocation ou installations sur site.
- Les zones Wavelength permettent aux développeurs de créer des applications qui offrent des latences ultra-faibles aux appareils 5G et aux utilisateurs finaux. Wavelength déploie des services de AWS calcul et de stockage standard à la périphérie des réseaux 5G des opérateurs de télécommunications.

AWS exploite state-of-the-art des centres de données hautement disponibles. Bien qu'elles soient rares, des pannes touchant la disponibilité des instances se trouvant au même emplacement peuvent se produire. Si vous hébergez toutes vos instances dans un seul emplacement touché par une panne, aucune de vos instances ne sera disponible.

Pour vous aider à déterminer le déploiement qui vous convient le mieux, consultez les [Questions fréquentes \(FAQ\)AWS Wavelength](#).

Table des matières

- [Régions](#)
- [Zones de disponibilité](#)
- [Zones locales](#)
- [Zones Wavelength](#)

- [AWS Outposts](#)

Régions

Chaque région est conçue pour être complètement isolée des autres régions . Cela permet d'atteindre la plus grande tolérance aux pannes possible et une stabilité optimale.

Lorsque vous consultez vos ressources, vous voyez uniquement celles liées à la région que vous avez spécifiée. Cela est dû au fait que les régions sont éloignées les unes des autres et que nous ne répliquons pas automatiquement les ressources entre régions.

Lorsque vous lancez une instance, vous devez sélectionner une AMI se trouvant dans la même région. Si l'AMI est dans une autre région, vous pouvez copier l'AMI dans la région que vous utilisez. Pour plus d'informations, consultez [Copier une AMI](#).

Notez qu'il n'y a pas de frais pour le transfert de données entre régions. Pour plus d'informations, consultez [Tarification Amazon EC2 - Transfert de données](#).

Sommaire

- [Régions disponibles](#)
- [Régions et points de terminaison](#)
- [Décrire vos régions](#)
- [Obtenir le nom d'affichage de la Région](#)
- [Spécifier la région pour une ressource](#)

Régions disponibles

Votre compte détermine les régions qui vous sont disponibles.

- An Compte AWS fournit plusieurs régions afin que vous puissiez lancer des instances Amazon EC2 dans des endroits qui répondent à vos besoins. Par exemple, vous pouvez souhaiter lancer des instances en Europe afin d'être plus proche de vos clients européens ou pour satisfaire à des exigences légales.
- Un compte AWS GovCloud (US-West) donne accès à la région AWS GovCloud (US-Ouest) et à la région AWS GovCloud (US-Est). Pour plus d'informations, consultez [AWS GovCloud \(US\)](#).
- Un compte Amazon AWS (Chine) permet d'accéder uniquement aux régions de Pékin et de Ningxia. Pour plus d'informations, veuillez consulter [Amazon Web Services en Chine](#).

Le tableau suivant répertorie les régions fournies par un Compte AWS. Vous ne pouvez pas décrire ou accéder à des régions supplémentaires à partir d'une région Compte AWS, telle que la AWS GovCloud (US) Regions ou les régions de Chine. Pour utiliser une région introduite après le 20 mars 2019, vous devez l'activer. Pour plus d'informations, voir [Spécifier les AWS régions que votre compte peut utiliser](#) dans le Guide de AWS Account Management référence.

Code	Nom	Statut d'inscription
us-east-2	USA Est (Ohio)	Facultatif
us-east-1	USA Est (Virginie)	Facultatif
us-west-1	USA Ouest (Californie du Nord)	Facultatif
us-west-2	USA Ouest (Oregon)	Facultatif
af-south-1	Afrique (Le Cap)	Obligatoire
ap-east-1	Asie-Pacifique (Hong Kong)	Obligatoire
ap-south-2	Asie-Pacifique (Hyderabad)	Obligatoire
ap-southeast-3	Asie-Pacifique (Jakarta)	Obligatoire
ap-southeast-4	Asie-Pacifique (Melbourne)	Obligatoire
ap-south-1	Asie-Pacifique (Mumbai)	Facultatif
ap-northeast-3	Asie-Pacifique (Osaka)	Facultatif
ap-northeast-2	Asie-Pacifique (Séoul)	Facultatif
ap-southeast-1	Asie-Pacifique (Singapour)	Facultatif
ap-southeast-2	Asie-Pacifique (Sydney)	Facultatif
ap-northeast-1	Asie-Pacifique (Tokyo)	Facultatif
ca-central-1	Canada (Centre)	Facultatif
ca-west-1	Canada Ouest (Calgary)	Obligatoire

Code	Nom	Statut d'inscription
eu-central-1	Europe (Francfort)	Facultatif
eu-west-1	Europe (Irlande)	Facultatif
eu-west-2	Europe (Londres)	Facultatif
eu-south-1	Europe (Milan)	Obligatoire
eu-west-3	Europe (Paris)	Facultatif
eu-south-2	Europe (Espagne)	Obligatoire
eu-north-1	Europe (Stockholm)	Facultatif
eu-central-2	Europe (Zurich)	Obligatoire
il-central-1	Israël (Tel Aviv)	Obligatoire
me-south-1	Moyen-Orient (Bahreïn)	Obligatoire
me-central-1	Moyen-Orient (EAU)	Obligatoire
sa-east-1	Amérique du Sud (São Paulo)	Facultatif

Pour plus d'informations, consultez [Infrastructure mondiale AWS](#).

Le nombre et le mappage des zones de disponibilité par région peut varier entre les Comptes AWS . Pour obtenir la liste des zones de disponibilité qui sont disponibles pour votre compte, vous pouvez utiliser la console Amazon EC2 ou l'interface de ligne de commande. Pour plus d'informations, consultez [Décrire vos régions](#).

Régions et points de terminaison

Lorsque vous utilisez une instance à l'aide de la CLI ou des actions d'API, vous devez spécifier son point de terminaison régional. Pour plus d'informations sur les régions et les points de terminaison d'Amazon EC2, consultez [Points de terminaison et quotas Amazon EC2](#) (français non garanti) dans le Référence générale d'Amazon Web Services.

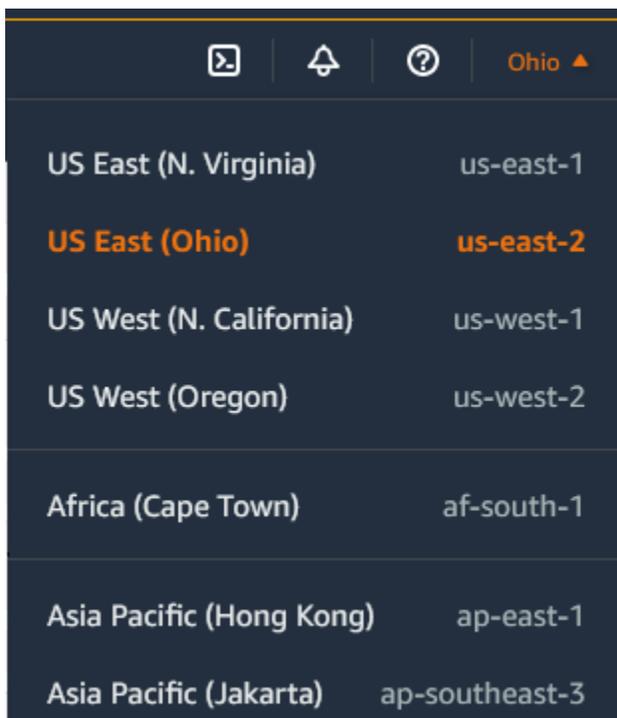
Pour plus d'informations sur les points de terminaison et les protocoles en AWS GovCloud (ouest des États-Unis), consultez la section [Points de terminaison de service](#) dans le guide de l'AWS GovCloud (US) utilisateur.

Décrire vos régions

Vous pouvez utiliser la console Amazon EC2 ou la CLI pour déterminer quelles régions et zones de disponibilité sont disponibles pour votre compte. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

Pour rechercher vos régions à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez le sélecteur Regions (Régions).



3. Vos ressources EC2 pour la Région sélectionnée sont affichées sur le tableau de bord EC2 dans la section Ressources.

Pour trouver vos régions à l'aide du AWS CLI

Utilisez la commande [describe-regions](#) comme suit pour décrire les régions qui sont activées pour votre compte.

```
aws ec2 describe-regions
```

Pour décrire toutes les régions, y compris celles qui sont désactivées pour votre compte, ajoutez l'option `--all-regions` comme suit.

```
aws ec2 describe-regions --all-regions
```

Obtenir le nom d'affichage de la Région

Vous pouvez utiliser le AWS Systems Manager Parameter Store pour afficher le nom d'affichage d'une région. Chaque Région possède des paramètres publics dans le chemin suivant.

```
/aws/service/global-infrastructure/regions/region-code
```

Les paramètres publics d'une Région sont les suivants :

- `/aws/service/global-infrastructure/regions/region-code/domain`
- `/aws/service/global-infrastructure/regions/region-code/geolocationCountry`
- `/aws/service/global-infrastructure/regions/region-code/geolocationRegion`
- `/aws/service/global-infrastructure/regions/region-code/longName`
- `/aws/service/global-infrastructure/regions/region-code/partition`

Le paramètre `longName` contient le nom d'affichage de la Région. La commande [get-parameters-by-path](#) suivante renvoie le nom d'affichage de la Région `af-south-1`. Elle utilise l'option `--query` pour étendre la sortie au nom de la Région. Vous devez placer la chaîne de requête entre guillemets simples sous Linux. Pour exécuter cette commande à l'aide de l'invite de commandes Windows, omettez les guillemets simples ou remplacez-les par des guillemets doubles.

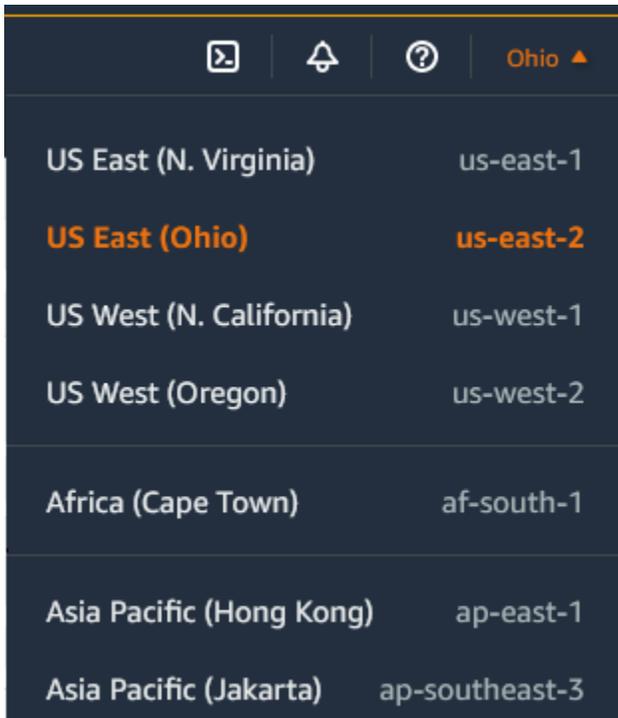
AWS CLI on Linux

```
aws ssm get-parameters-by-path \  
  --path /aws/service/global-infrastructure/regions/af-south-1 \  
  --query 'Parameters[?Name.contains(@, `longName`)].Value' \  
  --output text
```

AWS CLI on Windows

```
aws ssm get-parameters-by-path ^
```


2. Dans la barre de navigation, choisissez le sélecteur Regions (Régions), puis sélectionnez la région.



Pour spécifier la région par défaut à l'aide de la ligne de commande

Vous pouvez définir la valeur d'une variable d'environnement sur le point de terminaison régional souhaité (par exemple, `https://ec2.us-east-2.amazonaws.com`) :

- `AWS_DEFAULT_REGION` (AWS CLI)
- `Set-AWSDefaultRegion` (AWS Tools for Windows PowerShell)

L'autre solution consiste à utiliser l'option ligne de commande `--region` (AWS CLI) ou `-Region` (AWS Tools for Windows PowerShell) avec chaque commande individuelle. Par exemple, `--region us-east-2`.

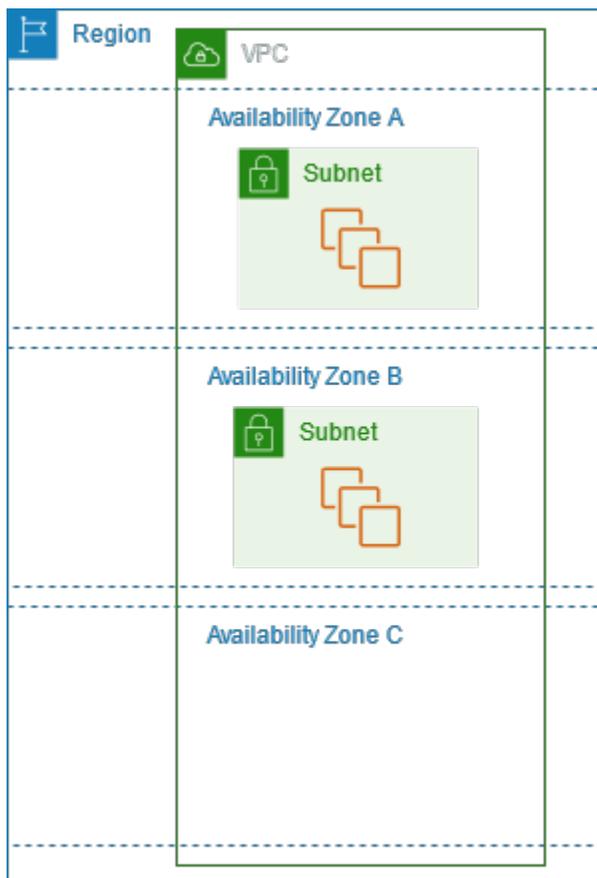
Pour plus d'informations sur les points de terminaison pour Amazon EC2, consultez la section Points de [terminaison et quotas Amazon EC2](#) dans le. Références générales AWS

Zones de disponibilité

Chaque région se compose de plusieurs emplacements isolés appelés zones de disponibilité. Le code de la zone de disponibilité est son code de Région suivi d'un identifiant à lettre. Par exemple, `us-east-1a`.

Lorsque vous lancez une instance, vous sélectionnez une Région et un cloud privé virtuel (VPC), puis vous pouvez sélectionner un sous-réseau dans l'une des zones de disponibilité ou nous laisser en choisir un pour vous. Si vous distribuez vos instances dans plusieurs zones de disponibilité et si une instance connaît une défaillance, vous pouvez concevoir votre application afin qu'une instance dans une autre zone de disponibilité puisse gérer les requêtes. Vous pouvez également utiliser les adresses IP Elastic pour masquer la défaillance d'une instance dans une zone de disponibilité en remappant rapidement l'adresse à une instance dans une autre zone de disponibilité.

Le schéma suivant illustre plusieurs zones de disponibilité dans une AWS région. La zone de disponibilité A et la zone de disponibilité B ont chacune un sous-réseau, et chaque sous-réseau possède des instances. La zone de disponibilité C n'a pas de sous-réseaux. Par conséquent, vous ne pouvez pas lancer d'instances dans cette zone de disponibilité.



Alors que les zones de disponibilité augmentent avec le temps, notre capacité à les développer peut devenir limitée. Dans ce cas, nous pouvons vous empêcher de lancer une instance dans une zone de disponibilité limitée, à moins que vous n'ayez déjà une instance dans cette zone de disponibilité. Finalement, nous pouvons également retirer la zone de disponibilité limitée de la liste des zones de disponibilité pour les nouveaux comptes. Par conséquent, votre compte peut avoir un nombre différent de zones de disponibilité disponibles dans une région qu'un autre compte.

Table des matières

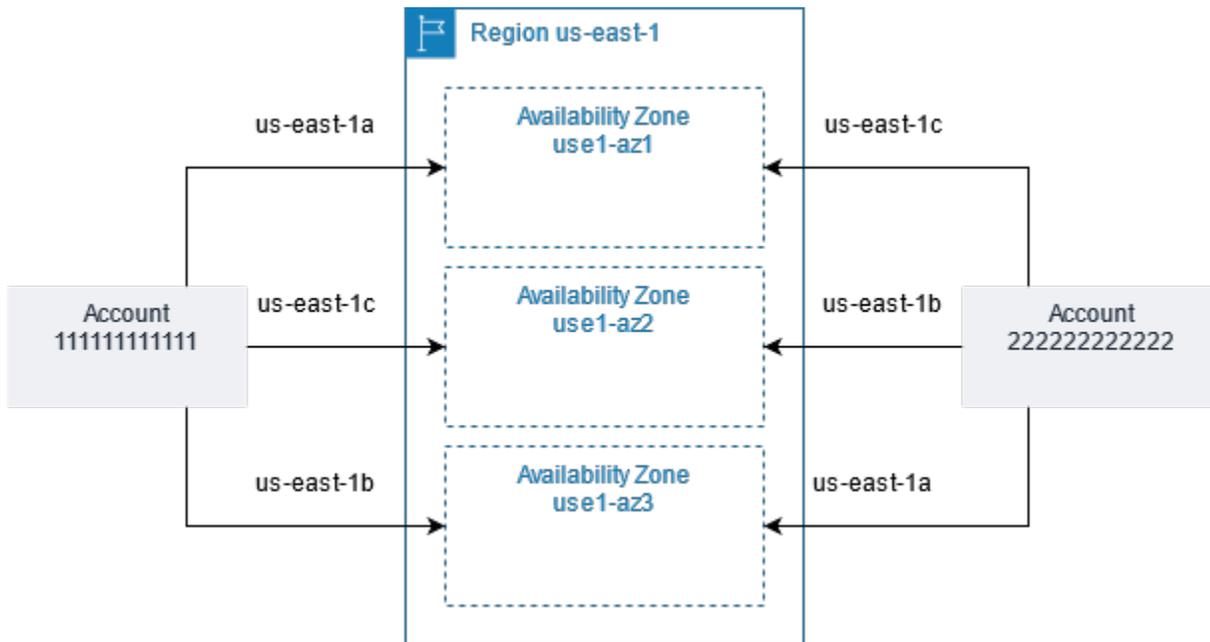
- [ID de zone de disponibilité](#)
- [Décrire vos zones de disponibilité](#)
- [Lancer des instances dans une zone de disponibilité](#)
- [Migrer une instance vers une autre zone de disponibilité](#)

ID de zone de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux codes de chacune Compte AWS de nos régions les plus anciennes. Par exemple, il se us-east-1a Compte AWS peut que votre emplacement physique ne soit pas le même que celui us-east-1a d'un autre Compte AWS.

Pour coordonner les zones de disponibilité entre les comptes de toutes les régions, même celles qui cartographient les zones de disponibilité, utilisez les ID AZ, qui sont des identifiants uniques et cohérents pour une zone de disponibilité. Par exemple, use1-az1 il s'agit d'un identifiant AZ pour la us-east-1 région, et il a le même emplacement physique dans chaque région Compte AWS. Vous pouvez afficher les ID des zones de disponibilité de votre compte afin de déterminer l'emplacement physique de vos ressources par rapport aux ressources d'un autre compte. Par exemple, si vous partagez avec un autre compte un sous-réseau dans la zone de disponibilité portant l'ID use1-az2, ce sous-réseau est accessible par cet autre compte dans la zone de disponibilité portant également l'ID use1-az2.

Le diagramme suivant illustre deux comptes avec des mappages différents entre le code de zone de disponibilité et l'ID de zone de disponibilité.



Décrire vos zones de disponibilité

Vous pouvez utiliser la console Amazon EC2 ou la CLI pour déterminer quelles zones de disponibilité sont disponibles pour votre compte. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

Pour rechercher vos zones de disponibilité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, choisissez le sélecteur Regions (Régions), puis sélectionnez la région.
3. Dans le panneau de navigation, choisissez Tableau de bord EC2.
4. Les zones de disponibilité sont répertoriées dans le panneau Service health (État du service).

Pour trouver vos zones de disponibilité à l'aide du AWS CLI

- Utilisez la commande [describe-availability-zones](#) comme suit pour décrire les zones de disponibilité dans la région spécifiée qui sont activées pour votre compte.

```
aws ec2 describe-availability-zones --region region-name
```

- Utilisez la commande [describe-availability-zones](#) comme suit pour décrire les zones de disponibilité, quel que soit leur statut d'inscription.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Lancer des instances dans une zone de disponibilité

Lorsque vous lancez une instance, sélectionnez une région qui rapproche vos instances de clients spécifiques, ou qui satisfait à vos exigences légales ou autres. En lançant vos instances dans des zones de disponibilité distinctes, vous pouvez protéger vos applications de la défaillance d'un emplacement unique.

Lorsque vous lancez une instance, vous pouvez éventuellement spécifier une zone de disponibilité dans la région que vous utilisez. Si vous ne spécifiez pas de zone de disponibilité, nous sélectionnons une zone de disponibilité pour vous. Lorsque vous lancez vos instances initiales, nous vous recommandons d'accepter la zone de disponibilité par défaut, car cela nous permet de sélectionner la meilleure zone de disponibilité pour vous, en fonction de l'état de santé du système et de la capacité disponible. Si vous lancez des instances additionnelles, ne spécifiez une zone de disponibilité que si vos nouvelles instances doivent être proches ou séparées de vos instances en cours d'exécution.

Migrer une instance vers une autre zone de disponibilité

Si nécessaire, vous pouvez migrer une instance d'une zone de disponibilité à une autre. Par exemple, si vous essayez de modifier le type d'instance de votre instance et que nous ne pouvons pas lancer une instance du nouveau type d'instance dans la zone de disponibilité actuelle, vous pouvez migrer l'instance vers une zone de disponibilité avec capacité pour le nouveau type d'instance.

Le processus de migration comporte les étapes suivantes :

- Création d'une AMI à partir de l'instance d'origine
- Lancement d'une instance dans la nouvelle zone de disponibilité
- Mise à jour de la configuration de la nouvelle instance, comme indiqué dans la procédure suivante

Pour migrer une instance vers une autre zone de disponibilité

1. Créez une AMI à partir de l'instance. La procédure dépend du type de volume de périphérique racine de l'instance. Pour plus d'informations, consultez la documentation correspondant au volume de votre périphérique racine :

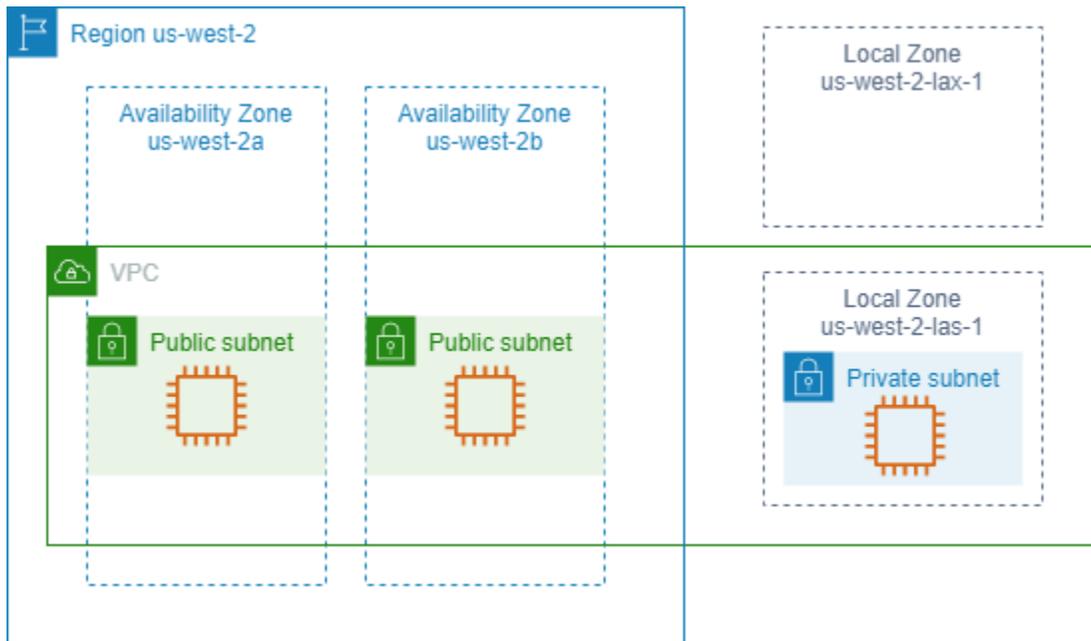
- [Création d'une AMI basée sur Amazon EBS](#)
 - [Créer une AMI Linux basée sur le stockage d'instance](#)
2. Si vous avez besoin de préserver l'adresse IPv4 privée d'une instance, vous devez supprimer le sous-réseau dans la zone de disponibilité actuelle, puis créer un sous-réseau dans la nouvelle zone de disponibilité avec la même plage d'adresses IPv4 que le sous-réseau d'origine. Veuillez noter que vous devez mettre fin à toutes les instances dans un sous-réseau avant de pouvoir le supprimer. Par conséquent, vous devez créer des AMI à partir de toutes les instances de votre sous-réseau de façon à pouvoir déplacer toutes les instances du sous-réseau actuel vers le nouveau sous-réseau.
 3. Lancez une instance depuis une AMI que vous avez créée, en spécifiant la nouvelle zone de disponibilité ou le nouveau sous-réseau. Vous pouvez utiliser le même type d'instance que pour l'instance d'origine ou sélectionner un nouveau type d'instance. Pour plus d'informations, consultez [Lancer des instances dans une zone de disponibilité](#).
 4. Si l'instance d'origine a une adresse IP Elastic associée, associez-la à la nouvelle instance. Pour plus d'informations, consultez [Dissocier une adresse IP Elastic](#).
 5. Si l'instance d'origine est une Instance réservée, changez la zone de disponibilité pour votre réservation. (Si vous avez également changé le type d'instance, vous pouvez aussi modifier le type d'instance de votre réservation). Pour plus d'informations, consultez [Soumettre des demandes de modification](#).
 6. (Facultatif) Mettez fin à l'instance d'origine. Pour plus d'informations, consultez [Résilier une instance](#).

Zones locales

Une zone locale est une extension d'une AWS région située à proximité géographique de vos utilisateurs. Les zones locales disposent de leurs propres connexions à Internet et de leur propre support AWS Direct Connect, de sorte que les ressources créées dans une zone locale peuvent servir les utilisateurs locaux avec des communications à faible latence. Pour plus d'informations, voir [Qu'est-ce que AWS les zones locales ?](#) dans le Guide de l'utilisateur des Zones AWS Locales.

Le code d'une zone locale est son code de Région suivi par un identifiant qui indique son emplacement physique. Par exemple, `us-west-2-lax-1` à Los Angeles.

Le schéma suivant illustre la AWS région us-west-2, deux de ses zones de disponibilité et deux de ses zones locales. Le VPC couvre les zones de disponibilité et l'une des zones locales. Chaque zone du VPC possède un sous-réseau et chaque sous-réseau possède une instance.



Pour utiliser une zone locale, vous devez d'abord l'activer. Pour plus d'informations, consultez [the section called "S'inscrire à Local Zones"](#). Créez ensuite un sous-réseau dans la zone locale. Enfin, lancez des ressources dans le sous-réseau de la zone locale, telles que des instances, afin que vos applications soient proches de vos utilisateurs.

Table des matières

- [Local Zones disponibles](#)
- [S'inscrire à Local Zones](#)
- [Lancez des instances dans une zone locale](#)

Local Zones disponibles

Vous pouvez utiliser la console Amazon EC2 ou une interface de ligne de commande pour déterminer les zones locales disponibles pour votre compte. Pour bénéficier d'une liste complète, consultez les [Emplacements de zones locales AWS](#).

Pour rechercher votre Local Zones à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans la barre de navigation, sélectionnez le sélecteur Regions (Régions), puis sélectionnez la région parente.
3. Dans le panneau de navigation, choisissez Tableau de bord EC2.
4. En haut à droite de la page, choisissez Attributs du compte, Zones.

Pour trouver vos Zones Locales à l'aide du AWS CLI

Utilisez la commande [describe-availability-zones](#) comme suit pour décrire toutes les zones locales dans la région spécifiée, même si elles ne sont pas activées. Pour décrire uniquement les zones locales que vous avez activées, omettez l'option `--all-availability-zones`.

```
aws ec2 describe-availability-zones --region region-name --filters Name=zone-type,Values=local-zone --all-availability-zones
```

S'inscrire à Local Zones

Avant de spécifier une zone locale pour une ressource ou un service, vous devez vous inscrire à Local Zones.

Considération

Certaines AWS ressources peuvent ne pas être disponibles dans toutes les régions. Assurez-vous que vous pouvez créer les ressources dont vous avez besoin dans les régions ou les Local Zones souhaitées avant de lancer une instance dans une zone locale spécifique. Pour connaître la liste des services pris en charge dans chaque zone locale, consultez les [Caractéristiques des zones locales AWS](#).

Pour vous inscrire à Local Zones à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le coin supérieur gauche de la page, sélectionnez Nouvelle expérience EC2. Vous ne pouvez pas exécuter cette tâche à l'aide de l'ancienne console.
3. Dans la barre de navigation, choisissez le sélecteur Regions (Régions), puis sélectionnez la région parente.
4. Dans le panneau de navigation, choisissez Tableau de bord EC2.
5. En haut à droite de la page, choisissez Attributs du compte, Zones.
6. Choisissez une zone locale, puis Action > Gérer le groupe de zones.

7. Sous État d'inscription, choisissez Activer.
8. Choisissez Mettre à jour.

Pour accéder aux Zones Locales à l'aide du AWS CLI

Utilisez la commande [modify-availability-zone-group](#).

Lancez des instances dans une zone locale

Lorsque vous lancez une instance, vous pouvez spécifier un sous-réseau qui se trouve dans une zone locale. Vous pouvez allouer une adresse IP à partir d'un groupe de frontières réseau. Un groupe de frontières réseau est un ensemble unique de zones de disponibilité, de Local Zones ou de zones Wavelength à partir desquelles AWS annonce des adresses IP, par exemple, `us-west-2-lax-1a`.

Vous pouvez allouer les adresses IP suivantes à partir d'un groupe de frontières réseau :

- Adresses IPv4 Elastic fournies par Amazon
- Adresses VPC IPv6 fournies par Amazon (disponibles uniquement dans les zones de Los Angeles)

Pour plus d'informations sur le lancement d'une instance dans une zone locale, consultez [Getting started with AWS Local Zones](#) dans le guide de l'utilisateur des zones AWS locales.

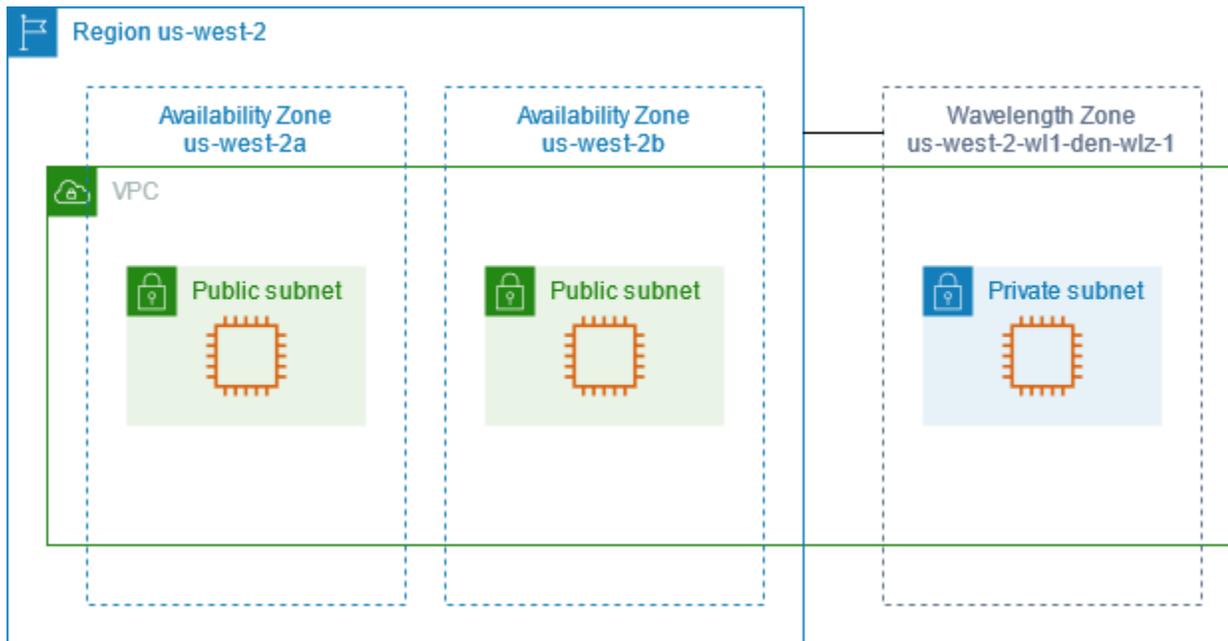
Zones Wavelength

AWS Wavelength permet aux développeurs de créer des applications offrant des latences extrêmement faibles aux appareils mobiles et aux utilisateurs finaux. Wavelength déploie des services de AWS calcul et de stockage standard à la périphérie des réseaux 5G des opérateurs de télécommunications. Les développeurs peuvent étendre un cloud privé virtuel (VPC) à une ou plusieurs zones de longueur d'onde, puis utiliser des AWS ressources telles que les instances Amazon EC2 pour exécuter des applications nécessitant une latence très faible et une connexion AWS aux services de la région.

Une zone Wavelength est une zone isolée située à l'emplacement du transporteur où l'infrastructure Wavelength est déployée. Les zones Wavelength sont liées à une région. Une zone Wavelength est une extension logique d'une région et est gérée par le plan de contrôle de la région.

Le code d'une zone Wavelength est son code de Région suivi par un identifiant qui indique son emplacement physique. Par exemple, `us-east-1-w11-bos-w1z-1` à Boston.

Le schéma suivant illustre la AWS région us-west-2, deux de ses zones de disponibilité et une zone Wavelength. Le VPC couvre les zones de disponibilité et la zone Wavelength. Chaque zone du VPC possède un sous-réseau et chaque sous-réseau possède une instance.



Pour utiliser une zone Wavelength, vous devez d'abord vous inscrire à la zone. Pour plus d'informations, consultez [the section called "Activer les zones Wavelength"](#). Ensuite, créez un sous-réseau dans la zone Wavelength. Enfin, lancez vos ressources dans le sous-réseau de zones Wavelength, afin que vos applications soient plus proches de vos utilisateurs finaux.

Les zones Wavelength ne sont pas disponibles dans toutes les régions. Pour plus d'informations sur les régions qui prennent en charge les zones Wavelength, consultez [Zones Wavelength disponibles](#) dans le Guide du développeur AWS Wavelength .

Sommaire

- [Décrire vos zones Wavelength](#)
- [Activer les zones Wavelength](#)
- [Lancer des instances dans une zone Wavelength](#)

Décrire vos zones Wavelength

Vous pouvez utiliser la console Amazon EC2 ou la CLI pour déterminer quelles zones Wavelength sont disponibles pour votre compte. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

Pour rechercher vos zones Wavelength à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, choisissez le sélecteur Regions (Régions), puis sélectionnez la région.
3. Dans le panneau de navigation, choisissez Tableau de bord EC2.
4. En haut à droite de la page, choisissez Attributs du compte, Zones.

Pour trouver vos zones de longueur d'onde à l'aide du AWS CLI

- Utilisez la commande [describe-availability-zones](#) comme suit pour décrire les zones Wavelength dans la région spécifiée qui sont activées pour votre compte.

```
aws ec2 describe-availability-zones --region region-name
```

- Utilisez la commande [describe-availability-zones](#) comme suit pour décrire les zones Wavelength, quel que soit leur statut d'inscription.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Activer les zones Wavelength

Avant de spécifier une zone Wavelength pour une ressource ou un service, vous devez vous inscrire à Zones Wavelength.

Considérations

- Certaines AWS ressources ne sont pas disponibles dans toutes les régions. Assurez-vous de pouvoir créer les ressources dont vous avez besoin dans la région ou la zone Wavelength souhaitée avant de lancer une instance dans une zone Wavelength spécifique.

Pour vous inscrire aux zones Wavelength à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le coin supérieur gauche de la page, sélectionnez Nouvelle expérience EC2. Vous ne pouvez pas exécuter cette tâche à l'aide de l'ancienne console.

3. Dans la barre de navigation, choisissez le sélecteur Regions (Régions), puis sélectionnez la région.
4. Dans le panneau de navigation, choisissez Tableau de bord EC2.
5. En haut à droite de la page, choisissez Attributs du compte, Zones.
6. Choisissez une zone de longueur d'onde, puis Action > Gérer le groupe de zones.
7. Sous État d'inscription, choisissez Activer.
8. Choisissez Mettre à jour.

Pour activer les zones de longueur d'onde à l'aide du AWS CLI

Utilisez la commande [modify-availability-zone-group](#).

Lancer des instances dans une zone Wavelength

Lorsque vous lancez une instance, vous pouvez spécifier un sous-réseau qui se trouve dans une zone Wavelength. Vous allouez également une adresse IP de transporteur à partir d'un groupe de frontières réseau, qui est un ensemble unique de zones de disponibilité, de Local Zones ou de zones Wavelength à partir desquelles AWS annonce des adresses IP, par exemple `us-east-1-w11-bos-w1z-1`.

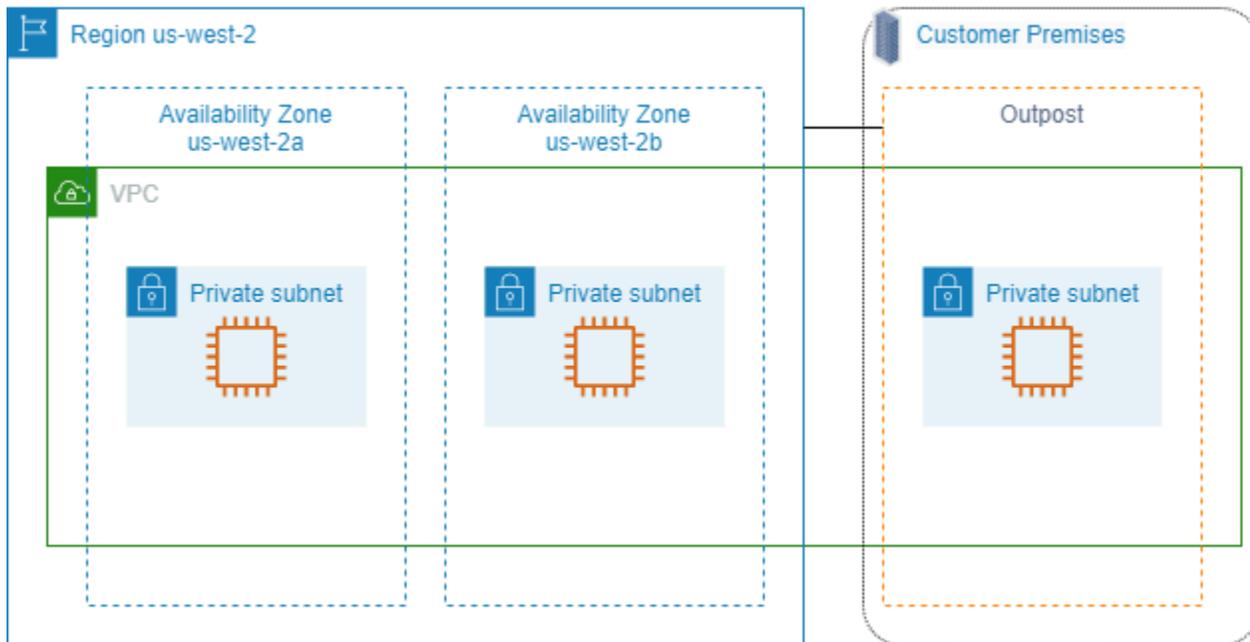
Pour plus d'informations sur le lancement d'une instance dans une zone Wavelength, consultez la section [Premiers pas avec AWS Wavelength](#) du Guide du développeur AWS Wavelength .

AWS Outposts

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructure, les services, les API et les outils aux locaux des clients. En fournissant un accès local à l'infrastructure AWS gérée, il AWS Outposts permet aux clients de créer et d'exécuter des applications sur site en utilisant les mêmes interfaces de programmation que dans AWS les régions, tout en utilisant les ressources de calcul et de stockage locales pour réduire la latence et les besoins de traitement des données locaux.

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région. Vous pouvez créer des sous-réseaux sur votre Outpost et les spécifier lorsque vous créez des AWS ressources. Les instances des sous-réseaux Outpost communiquent avec d'autres instances de la AWS région à l'aide d'adresses IP privées, le tout au sein du même VPC.

Le schéma suivant illustre la AWS région us-west-2, deux de ses zones de disponibilité et un avant-poste. Le VPC couvre les zones de disponibilité et l'Outpost. L'Outpost se trouve dans un centre de données client sur site. Chaque zone du VPC possède un sous-réseau et chaque sous-réseau possède une instance.



Pour commencer à utiliser AWS Outposts, vous devez créer un avant-poste et commander une capacité d'avant-poste. Pour plus d'informations sur les configurations outposts, consultez [notre catalogue](#). Une fois votre équipement Outpost installé, la capacité de calcul et de stockage est disponible pour vous lorsque vous lancez des instances Amazon EC2 sur votre Outpost.

Lancer des instances sur un outpost

Vous pouvez lancer des instances EC2 dans le sous-réseau outpost que vous avez créé. Les groupes de sécurité contrôlent le trafic entrant et sortant pour les instances avec des interfaces réseau Elastic dans un sous-réseau Outpost, comme ils le font pour les instances dans un sous-réseau de zone de disponibilité. Pour vous connecter à une instance EC2 dans un sous-réseau outpost, vous pouvez spécifier une paire de clés lorsque vous lancez l'instance, comme vous le faites pour les instances d'un sous-réseau de zone de disponibilité.

Nous vous recommandons de limiter le volume racine d'une instance sur un rack Outpost à 30 GiB ou moins. Vous pouvez spécifier des volumes de données dans le mappage de périphériques de blocs de l'AMI ou de l'instance pour fournir un stockage supplémentaire. Pour supprimer les blocs inutilisés du volume de démarrage, consultez la section [Comment créer des volumes EBS épars](#) sur le blog du réseau de AWS partenaires.

Nous vous recommandons d'augmenter le délai d'attente de NVMe pour le volume racine. Pour plus d'informations, consultez la section [Délai d'expiration des opérations d'E/S](#).

Pour plus d'informations sur la création d'un Outpost, consultez la section [Premiers pas avec AWS Outposts](#) du Guide de l'utilisateur AWS Outposts .

Création d'un volume sur un rack Outpost

AWS Outposts propose des formats rack et serveur. Si votre capacité se trouve sur un rack Outpost, vous pouvez créer des volumes EBS dans le sous-réseau Outpost que vous avez créé. Lorsque vous créez le volume, spécifiez l'Amazon Resource Name (ARN) de l'outpost.

La commande [create-volume](#) suivante crée un volume vide de 50 Go sur l'outpost spécifié.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

Vous pouvez modifier dynamiquement la taille de vos volumes gp2 Amazon EBS sans les détacher. Pour plus d'informations sur la modification d'un volume sans le détacher, voir [Demander des modifications à vos volumes EBS](#).

Adressage IP des instances Amazon EC2

Amazon EC2 et Amazon VPC prennent en charge les protocoles d'adressage IPv4 et IPv6. Par défaut, Amazon VPC utilise le protocole d'adressage IPv4 ; vous ne pouvez pas désactiver ce comportement. Lorsque vous créez un VPC, vous devez spécifier un bloc d'adresses CIDR IPv4 (une plage d'adresses IPv4 privées). Vous pouvez éventuellement attribuer un bloc d'adresse CIDR IPv6 à votre VPC et attribuer des adresses IPv6 de ce bloc aux instances de vos sous-réseaux.

Table des matières

- [Adresses IPv4 privées](#)
- [Adresses IPv4 publiques](#)
- [Optimisation des adresses IPv4 publiques](#)
- [Adresses IP Elastic \(IPv4\)](#)
- [Adresses IPv6](#)
- [Utiliser les adresses IPv4 pour vos instances](#)
- [Utiliser les adresses IPv6 pour vos instances](#)
- [Plusieurs adresses IP pour vos instances EC2](#)

- [Configurer une adresse IPv4 privée secondaire pour votre instance Windows](#)
- [Noms d'hôtes d'instance EC2](#)
- [Adresses lien-local](#)

Adresses IPv4 privées

Une adresse IPv4 privée est une adresse IP qui ne peut pas être atteinte via Internet. Vous pouvez utiliser des adresses IPv4 privées et un nom d'hôte DNS interne pour toute communication entre des instances du même VPC. Pour plus d'informations sur les normes et spécifications des adresses IPv4 privées, consultez [RFC 1918](#). Nous allouons des adresses IPv4 privées aux instances à l'aide de DHCP.

Note

Vous pouvez créer un VPC avec un bloc d'adresses CIDR publiquement routable ne faisant pas partie des plages d'adresses IPv4 privées spécifiées dans la norme RFC 1918. Toutefois, dans le cadre de cette documentation, nous faisons référence à des adresses IPv4 privées (ou « adresses IP privées ») en tant qu'adresses IP se trouvant dans la plage CIDR IPv4 de votre VPC.

Les sous-réseaux VPC peuvent être de l'un des types suivants :

Les sous-réseaux VPC peuvent être de l'un des types suivants :

- Sous-réseaux exclusivement IPv4 : vous ne pouvez créer des ressources dans ces sous-réseaux que si des adresses IPv4 leur sont attribuées.
- Sous-réseaux exclusivement IPv6 : vous ne pouvez créer des ressources dans ces sous-réseaux que si des adresses IPv6 leur sont attribuées.
- Sous-réseaux IPv4 et IPv6 : vous pouvez créer des ressources dans ces sous-réseaux avec des adresses IPv4 ou IPv6 qui leur sont attribuées.

Lorsque vous lancez une instance EC2 dans un sous-réseau exclusivement IPv4 ou à double pile (IPv4 et IPv6), l'instance reçoit une adresse IP privée primaire de la plage d'adresses IPv4 du sous-réseau. Pour plus d'informations, consultez la section [IP addressing](#) (Adressage IP) dans le Guide de l'utilisateur Amazon VPC. Si vous ne spécifiez pas d'adresse IP privée principale lorsque vous lancez l'instance, nous sélectionnons une adresse IP disponible dans la plage IPv4 de sous-réseaux

à votre place. Chaque instance d'un VPC comporte une interface réseau par défaut (eth0) à laquelle une adresse IPv4 privée principale est attribuée. Vous pouvez également spécifier des adresses IPv4 privées supplémentaires, connues sous le nom d'adresses IPv4 privées secondaires. Contrairement aux adresses IP privées principales, les adresses IP privées secondaires peuvent être réaffectées d'une instance à une autre. Pour plus d'informations, consultez [Plusieurs adresses IP pour vos instances EC2](#).

Qu'il s'agisse d'une adresse principale ou secondaire, une adresse IPv4 privée reste associée à l'interface réseau lorsque l'instance est arrêtée (ou mise en veille) et redémarrée, ainsi que lorsqu'elle est libérée lors de la désactivation de l'instance.

Adresses IPv4 publiques

Une adresse IP publique est une adresse IPv4, qui est accessible depuis Internet. Vous pouvez utiliser des adresses publiques pour les communications entre vos instances et Internet.

Lorsque vous lancez une instance dans un VPC par défaut, nous lui attribuons une adresse IP publique par défaut. Lorsque vous lancez une instance sur un VPC autre qu'un VPC par défaut, le sous-réseau a un attribut qui détermine si les instances lancées sur ce sous-réseau reçoivent une adresse IP publique à partir du groupe d'adresses IPv4 publiques. Par défaut, nous n'attribuons aucune adresse IP publique aux instances lancées dans un sous-réseau autre que celui défini par défaut.

Vous pouvez contrôler si votre instance reçoit une adresse IP publique en procédant comme suit :

- Modifier l'attribut d'adressage IP public de votre sous-réseau. Pour plus d'informations, consultez la section [Modifier l'attribut d'adressage IPv4 public de votre sous-réseau](#) dans le Guide de l'utilisateur Amazon VPC.
- Activer ou désactiver la fonction d'adressage IP public pendant le lancement, ce qui remplace l'attribut d'adressage IP public du sous-réseau. Pour plus d'informations, consultez [Attribuer une adresse IPv4 publique lors du lancement d'une instance](#).
- Vous pouvez annuler l'attribution d'une adresse IP publique à votre instance après le lancement en [gérant les adresses IP associées à une interface réseau](#).

Une adresse IP publique est attribuée à votre instance à partir du pool d'adresses IPv4 publiques d'Amazon et n'est pas associée à votre AWS compte. Quand une adresse IP publique est dissociée de votre instance, elle est réintégrée dans le pool d'adresses IPv4 publiques et vous ne pouvez plus la réutiliser.

Dans certains cas, nous publions l'adresse IP publique de votre instance ou nous lui en attribuons une nouvelle :

- Nous libérons l'adresse IP publique de votre instance lorsqu'elle est arrêtée, mise en veille ou mise hors service. Toute instance arrêtée ou mise en veille de manière prolongée reçoit une nouvelle adresse IP publique au démarrage.
- L'adresse IP publique de votre instance est libérée lorsque vous lui associez une adresse IP Elastic. Lorsque vous dissociez l'adresse IP Elastic de votre instance, cette dernière reçoit une nouvelle adresse IP publique.
- Si l'adresse IP publique de votre instance sur un VPC a été libérée, cette instance ne recevra pas de nouvelle adresse si plusieurs interfaces réseau sont attachées à l'instance.
- Si l'adresse IP publique de votre instance est libérée alors qu'elle a une adresse IP privée secondaire associée à une adresse IP Elastic, l'instance ne reçoit pas de nouvelle adresse IP publique.

Si vous avez besoin d'une adresse IP publique permanente qui peut être associée aux instances et en être dissociée comme vous le souhaitez, utilisez plutôt une adresse IP Elastic.

Si vous utilisez DNS dynamique pour mapper un nom DNS existant à l'adresse IP publique d'une nouvelle instance, cela peut prendre jusqu'à 24 heures pour que l'adresse IP soit propagée via Internet. De ce fait, de nouvelles instances peuvent ne pas recevoir le trafic alors que des instances terminées continuent de recevoir des demandes. Pour résoudre ce problème, utilisez une adresse IP Elastic. Vous pouvez allouer votre propre adresse IP Elastic, puis l'associer à votre instance. Pour plus d'informations, consultez [Adresses IP Elastic](#).

Note

- AWS frais pour toutes les adresses IPv4 publiques, y compris les adresses IPv4 publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet Adresse IPv4 publique de la [page de tarification d'Amazon VPC](#).
- Les instances qui accèdent à d'autres instances via leur adresse IP NAT publique doivent régler le transfert de données régional ou Internet (selon que les instances se trouvent dans la même région ou non).

Optimisation des adresses IPv4 publiques

AWS frais pour toutes les adresses IPv4 publiques, y compris les adresses IPv4 publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet Adresse IPv4 publique de la [page de tarification d'Amazon VPC](#).

La liste suivante contient les actions que vous pouvez entreprendre pour optimiser le nombre d'adresses IPv4 publiques que vous utilisez :

- Utilisez un [équilibreur de charge élastique](#) pour équilibrer la charge du trafic vers vos instances EC2 et [désactivez l'attribution automatique d'une adresse IP publique sur l'ENI principal attribué aux instances](#). Les équilibreurs de charge utilisent une seule adresse IPv4 publique, ce qui réduit le nombre d'adresses IPv4 publiques. Vous souhaitez peut-être également consolider les équilibreurs de charge existants afin de réduire davantage le nombre d'adresses IPv4 publiques.
- Si la seule raison d'utiliser une passerelle NAT est de se connecter par SSH à une instance EC2 dans un sous-réseau privé pour des raisons de maintenance ou d'urgence, envisagez plutôt d'utiliser le point de terminaison [EC2 Instance Connect](#). Avec EC2 Instance Connect Endpoint, vous pouvez vous connecter à une instance depuis Internet sans que celle-ci ait besoin d'une adresse IPv4 publique.
- Si vos instances EC2 se trouvent dans un sous-réseau public auquel des adresses IP publiques leur sont attribuées, envisagez de les déplacer vers un sous-réseau privé, de supprimer les adresses IP publiques et d'utiliser une [passerelle NAT publique](#) pour autoriser l'accès à vos instances EC2 et depuis celles-ci. L'utilisation de passerelles NAT comporte des considérations financières. Utilisez cette méthode de calcul pour déterminer si les passerelles NAT sont rentables. Vous pouvez obtenir les informations Number of public IPv4 addresses nécessaires à ce calcul en [créant un rapport sur les coûts AWS de facturation et l'utilisation](#).

```
NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing public IP cost
```

Où :

- NAT gateway per hour = $\$0.045 * 730 \text{ hours in a month} * \text{Number of Availability Zones the NAT gateways are in}$
- NAT gateway public IPs = $\$0.005 * 730 \text{ hours in a month} * \text{Number of IPs associated with your NAT gateways}$
- NAT gateway transfer = $\$0.045 * \text{Number of GBs that will go through the NAT gateway in a month}$

- Existing public IP cost = $\$0.005 * 730 \text{ hours in a month} * \text{Number of public IPv4 addresses}$

Si le total est inférieur à 1, les passerelles NAT sont moins chères que les adresses IPv4 publiques.

- Utilisez-le [AWS PrivateLink](#) pour vous connecter en privé à AWS des services ou à des services hébergés par d'autres AWS comptes plutôt que d'utiliser des adresses IPv4 publiques et des passerelles Internet.
- [Apportez votre propre plage d'adresses IP \(BYOIP\) AWS et utilisez-la](#) pour les adresses IPv4 publiques plutôt que d'utiliser des adresses IPv4 publiques appartenant à Amazon.
- Désactivez l'[attribution automatique d'une adresse IPv4 publique pour les instances lancées dans des sous-réseaux](#). Cette option est généralement désactivée par défaut pour les VPC lorsque vous créez un sous-réseau, mais vous devez vérifier vos sous-réseaux existants pour vous assurer qu'elle est désactivée.
- Si vous avez des instances EC2 qui n'ont pas besoin d'adresses IPv4 publiques, [vérifiez que l'attribution automatique d'une adresse IP publique est désactivée sur les interfaces réseau associées à vos instances](#).
- [Configurez les points de terminaison de l'accélérateur AWS Global Accelerator](#) pour les instances EC2 dans des sous-réseaux privés afin de permettre au trafic Internet de circuler directement vers les points de terminaison de vos VPC sans avoir besoin d'adresses IP publiques. Vous pouvez également [apporter vos propres adresses AWS Global Accelerator et utiliser](#) vos propres adresses IPv4 pour les adresses IP statiques de votre accélérateur.

Adresses IP Elastic (IPv4)

Une adresse IP Elastic est une adresse IPv4 publique que vous pouvez allouer à votre compte. Vous pouvez l'associer à des instances et le dissocier selon vos besoins. Elle est allouée à votre compte jusqu'à ce que vous choisissiez de la libérer. Pour plus d'informations sur les adresses IP Elastic et leur utilisation, consultez [Adresses IP Elastic](#).

Nous ne prenons pas en charge les adresses IP Elastic pour IPv6.

Adresses IPv6

Le cas échéant, vous pouvez associer un bloc d'adresses CIDR IPv6 à votre VPC, et associer les blocs d'adresse CIDR IPv6 à vos sous-réseaux. Le bloc d'adresses CIDR IPv6 de votre VPC est

automatiquement attribué à partir du pool d'adresses IPv6 d'Amazon ; vous ne pouvez pas choisir la plage vous-même. Pour plus d'informations, consultez les rubriques suivantes dans le Amazon VPC Guide de l'utilisateur :

- [Adressage IP pour vos VPC et sous-réseaux](#)
- [Ajout d'un bloc d'adresse CIDR IPv6 à votre VPC](#)
- [Ajout d'un bloc d'adresse CIDR IPv6 à votre sous-réseau](#)

Les adresses IPv6 sont globalement uniques et peuvent être configurées pour rester privées ou être accessibles via Internet. Votre instance reçoit une adresse IPv6 si un bloc d'adresses CIDR IPv6 est associé à votre VPC et votre sous-réseau, et si l'une des conditions suivantes est vraie :

- Votre sous-réseau est configuré pour attribuer automatiquement une adresse IPv6 à une instance lors du lancement. Pour plus d'informations, consultez [Modifier l'attribut d'adressage IPv6 public de votre sous-réseau](#).
- Vous attribuez une adresse IPv6 à votre instance lors du lancement.
- Vous attribuez une adresse IPv6 à l'interface réseau principale de votre instance après son lancement.
- Vous attribuez une adresse IPv6 à une interface réseau dans le même sous-réseau et vous liez l'interface réseau à votre instance après son lancement.

Lorsque votre instance reçoit une adresse IPv6 lors du lancement, l'adresse est associée à l'interface réseau principale (eth0) de l'instance. Vous pouvez gérer les adresses IPv6 pour l'interface réseau principale de vos instances (eth0) comme suit :

- Attribution et annulation de l'attribution d'adresses IPv6 de l'interface réseau. Le nombre d'adresses IPv6 que vous pouvez assigner à une interface réseau et le nombre d'interfaces réseau que vous pouvez lier à une instance varient en fonction du type d'instance. Pour plus d'informations, consultez [Adresses IP par interface réseau et par type d'instance](#).
- Activez une adresse IPv6 principale. Une adresse IPv6 principale vous permet d'éviter de perturber le trafic vers les instances ou les ENI. Pour plus d'informations, consultez [Créer une interface réseau](#) ou [Gérer les adresses IP](#).

Une adresse IPv6 persiste lorsque vous arrêtez (ou mettez en veille) et démarrez votre instance, et est libérée lorsque vous désactivez votre instance. Vous ne pouvez pas réattribuer une adresse IPv6 si elle est déjà attribuée à une autre interface réseau — vous devez d'abord annuler l'attribution.

Vous pouvez contrôler si les instances sont accessibles via leurs adresses IPv6 en contrôlant le routage de votre sous-réseau, ou à l'aide des règles ACL réseau et de groupe de sécurité. Pour de plus amples informations, veuillez consulter la section [Confidentialité du trafic inter-réseau](#) du Guide de l'utilisateur Amazon VPC.

Pour plus d'informations sur les plages d'adresses IPv6 réservées, consultez [Registre d'adresses IPv6 IANA à des fins spéciales](#) et [RFC4291](#).

Utiliser les adresses IPv4 pour vos instances

Vous pouvez attribuer une adresse IPv4 publique à votre instance lorsque vous la lancez. Vous pouvez afficher les adresses IPv4 de votre dans la console via la page Instances ou la page Interfaces réseau.

Table des matières

- [Afficher les adresses IPv4](#)
- [Attribuer une adresse IPv4 publique lors du lancement d'une instance](#)

Afficher les adresses IPv4

Vous pouvez utiliser la console Amazon EC2 afin d'afficher les adresses IPv4 publiques et privées de vos instances. Vous pouvez également déterminer les adresses IPv4 publiques et privées de votre instance depuis cette dernière en utilisant ses métadonnées. Pour plus d'informations, consultez [Utiliser des métadonnées d'instance](#).

L'adresse IPv4 publique est affichée comme propriété de l'interface réseau dans la console, mais elle est mappée à l'adresse IPv4 privée principale via la traduction d'adresses réseau (NAT, Network Address Translation). Par conséquent, si vous inspectez les propriétés de votre interface réseau sur votre instance, par exemple via `ifconfig` (Linux) ou `ipconfig` (Windows), l'adresse IPv4 publique ne s'affiche pas. Pour déterminer l'adresse IPv4 publique de votre instance à partir d'une instance, utilisez les métadonnées d'instance.

Pour afficher les adresses IPv4 d'une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel [Accès à Amazon EC2](#).

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).

Pour déterminer les adresses IPv4 publiques de votre instance à l'aide de ses métadonnées

1. Connectez-vous à votre instance. Pour plus d'informations, consultez [Connectez-vous à votre instance EC2](#).
2. Utilisez la commande suivante pour accéder à l'adresse IP privée.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/local-ipv4
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4
```

Tools for Windows PowerShell

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
```

3. Utilisez la commande suivante pour accéder à l'adresse IP publique. Notez que si une adresse IP Elastic est associée à l'instance, la valeur renvoyée est celle de l'adresse IP Elastic.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-ipv4
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-ipv4
```

Tools for Windows PowerShell

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
```

Attribuer une adresse IPv4 publique lors du lancement d'une instance

Chaque sous-réseau a un attribut qui détermine si une adresse IP publique est attribuée aux instances lancées dans ce sous-réseau. Par défaut, cet attribut est configuré sur `false` pour les sous-réseaux personnalisés et sur `true` pour les sous-réseaux par défaut. Lorsque vous lancez une instance, une fonction d'adressage IPv4 public vous permet également de vérifier si votre instance dispose d'une adresse IPv4 publique. Vous pouvez remplacer le comportement par défaut de l'attribut d'adressage IP du sous-réseau. L'adresse IPv4 publique est attribuée à partir du pool d'adresses IPv4 publiques d'Amazon, et est attribuée à l'interface réseau avec l'index du périphérique `eth0`. Cette fonction dépend de certaines conditions au moment du lancement de votre instance.

Considérations

- Vous pouvez annuler l'attribution de l'adresse IP publique à votre instance après le lancement en [gérant les adresses IP associées à une interface réseau](#). Pour plus d'informations sur les adresses IPv4 publiques, consultez [Adresses IPv4 publiques](#).
- Vous ne pouvez pas attribuer automatiquement une adresse IP publique si vous spécifiez plusieurs interfaces réseau. En outre, vous ne pouvez pas remplacer le paramètre de sous-réseau à l'aide de la fonction « auto-assign IP public », si vous spécifiez une interface réseau existante pour `eth0`.
- Que vous attribuez une adresse IP publique à votre instance lors du lancement ou non, vous pouvez associer une adresse IP élastique à votre instance après son lancement. Pour plus d'informations, consultez [Adresses IP Elastic](#). Vous pouvez également modifier le comportement de l'adressage IPv4 public de votre sous-réseau. Pour plus d'informations, consultez la section [Modifier l'attribut d'adressage IPv4 public de votre sous-réseau](#).

Pour attribuer une adresse IPv4 publique lors du lancement d'une instance à l'aide de la console

Suivez la procédure décrite pour [lancer une instance](#), et lorsque vous configurez les [Paramètres réseau](#), choisissez l'option Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique).

Pour activer ou désactiver la fonctionnalité d'adressage IP publique à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- Utilisez l'option `--associate-public-ip-address` ou `--no-associate-public-ip-address` avec la commande [run-instances](#) (AWS CLI)
- Utilisez le `-AssociatePublicIp` paramètre avec la [New-EC2Instance](#) commande (AWS Tools for Windows PowerShell)

Utiliser les adresses IPv6 pour vos instances

Vous pouvez afficher les adresses IPv6 affectées à votre instance, attribuer une adresse IPv6 publique à votre instance ou annuler l'affectation d'une adresse IPv6 à votre instance. Vous pouvez afficher ces adresses dans la console via la page Instances ou la page Interfaces réseau.

Sommaire

- [Afficher les adresses IPv6](#)
- [Attribuer une adresse IPv6 à une instance](#)
- [Annuler l'attribution d'une adresse IPv6 à partir d'une instance](#)

Afficher les adresses IPv6

Vous pouvez utiliser la console Amazon EC2 et les métadonnées AWS CLI des instances pour afficher les adresses IPv6 de vos instances.

Pour afficher les adresses IPv6 d'une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Sous l'onglet Mise en réseau, recherchez les adresses IPv6.

Pour afficher les adresses IPv6 d'une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel [Accès à Amazon EC2](#).

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).

Pour afficher les adresses IPv6 d'une instance à l'aide de métadonnées d'instance

1. Connectez-vous à votre instance. Pour plus d'informations, consultez [Connectez-vous à votre instance EC2](#).
2. Obtenez l'adresse MAC de l'instance auprès de `http://169.254.169.254/latest/meta-data/network/interfaces/macs/`.
3. Utilisez la commande suivante pour afficher l'adresse IPv6.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
```

Tools for Windows PowerShell

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
```

Attribuer une adresse IPv6 à une instance

Si votre VPC et votre sous-réseau disposent de blocs d'adresse CIDR IPv6 associés, vous pouvez attribuer une adresse IPv6 à votre instance pendant ou après le lancement. L'adresse IPv6 publique

est attribuée à partir de plage d'adresses IPv6 publiques du sous-réseau à l'interface réseau avec l'index du périphérique eth0.

Pour attribuer une adresse IPv6 lors du lancement d'une instance

Suivez la procédure décrite pour [lancer une instance](#), et lorsque vous configurez les [paramètres réseau](#), choisissez l'option pour Auto-assign IPv6 IP (Attribuer automatiquement l'adresse IPv6).

Pour attribuer une adresse IPv6 après son lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez votre instance et choisissez Actions, Mise en réseau, puis Gérer les adresses IP privées.
4. Sélectionnez l'interface réseau. Sous Adresses IPv6, choisissez Attribuer une nouvelle adresse IP. Entrez une adresse IPv6 de la plage du sous-réseau ou laissez le champ vide pour permettre à Amazon de choisir une adresse IPv6 pour vous.
5. Choisissez Enregistrer.

Pour attribuer une adresse IPv6 à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- Utilisez l'option `--ipv6-addresses` avec la commande [run-instances](#) (AWS CLI)
- Utilisez la `Ipv6Addresses` propriété for `-NetworkInterface` dans la [New-EC2Instance](#) commande (AWS Tools for Windows PowerShell)
- [assign-ipv6-addresses](#) (AWS CLI)
- `Register-EC2IpvAddressList`([6](#)AWS Tools for Windows PowerShell)

Annuler l'attribution d'une adresse IPv6 à partir d'une instance

Vous pouvez à tout moment annuler l'affectation d'une adresse IPv6 à partir d'une instance.

Pour annuler l'affectation d'une adresse IPv6 à une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.

3. Sélectionnez votre instance et choisissez Actions, Mise en réseau, puis Gérer les adresses IP privées.
4. Sélectionnez l'interface réseau. Sous Adresses IPv6, choisissez Annuler l'attribution en regard de l'adresse IPv6.
5. Choisissez Enregistrer.

Pour annuler l'affectation d'une adresse IPv6 à une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [unassign-ipv6-addresses](#) (AWS CLI)
- `Unregister-EC2Ipv6AddressList` (AWS Tools for Windows PowerShell).

Plusieurs adresses IP pour vos instances EC2

Vous pouvez spécifier plusieurs adresses IPv4 et IPv6 privées pour vos instances. Le nombre d'interfaces réseau et d'adresses IPv4 et IPv6 privées que vous pouvez spécifier pour une instance dépend du type d'instance. Pour plus d'informations, consultez [Adresses IP par interface réseau et par type d'instance](#).

Il peut être utile d'attribuer plusieurs adresses IP privées à une instance sur votre VPC pour effectuer les opérations suivantes :

- Héberger plusieurs sites web sur un seul serveur en utilisant plusieurs certificats SSL sur un seul serveur et en associant chaque certificat à une adresse IP spécifique.
- Faire fonctionner les composants des réseaux tels que les pare-feu ou les équilibreurs de charge qui ont plusieurs adresses IP pour chaque interface réseau.
- Rediriger le trafic interne vers une instance de secours en cas d'échec de votre instance, en réattribuant l'adresse IP secondaire à l'instance de secours.

Sommaire

- [Utilisation de plusieurs adresses IP](#)
- [Utiliser plusieurs adresses IPv4](#)
- [Utiliser plusieurs adresses IPv6](#)

Utilisation de plusieurs adresses IP

La liste suivante explique le fonctionnement de plusieurs adresses IP avec les interfaces réseau :

- Vous pouvez attribuer une adresse IPv4 privée secondaire à n'importe quelle interface réseau.
- Vous pouvez attribuer plusieurs adresses IPv6 à une interface réseau qui se trouve dans un sous-réseau disposant d'un bloc d'adresses CIDR IPv6 associé.
- Vous devez choisir une adresse IPv4 secondaire à partir de la plage du bloc d'adresses CIDR IPv4 du sous-réseau pour l'interface réseau.
- Vous devez choisir les adresses IPv6 à partir de la plage du bloc d'adresses CIDR IPv6 du sous-réseau de l'interface réseau.
- Vous associez des groupes de sécurité aux interfaces réseau, pas d'adresses IP individuelles. Par conséquent, chaque adresse IP que vous spécifiez dans une interface réseau est soumise au groupe de sécurité de son interface réseau.
- Plusieurs adresses IP peuvent être attribuées aux interfaces réseau liées aux instances en cours d'exécution ou arrêtées, ou leur attribution à ces interfaces peut être annulée.
- Les adresses IPv4 privées secondaires attribuées à une interface réseau peuvent être réattribuées à une autre interface si vous l'autorisez explicitement.
- Une adresse IPv6 ne peut pas être réattribuée à une autre interface réseau ; vous devez tout d'abord annuler l'attribution de l'adresse IPv6 à partir de l'interface réseau existante.
- Lorsque vous attribuez plusieurs adresses IP à une interface réseau à l'aide des outils ou de l'API de ligne de commande, l'opération complète échoue si l'une des adresses IP ne peut pas être attribuée.
- Les adresses IPv4 privées principales, les adresses IPv4 privées secondaires, les adresses IP Elastic et les adresses IPv6 restent avec une interface réseau secondaire lorsque celle-ci est dissociée d'une instance ou attachée à une instance.
- Même si vous ne pouvez pas détacher l'interface réseau principale à partir d'une instance, vous pouvez réattribuer l'adresse IPv4 privée secondaire de l'interface réseau principale à une autre interface réseau.

La liste suivante explique le fonctionnement de plusieurs adresses IP avec les adresses IP Elastic (IPv4 uniquement) :

- Chaque adresse IPv4 privée peut être associée à une seule adresse IP Elastic, et inversement.

- Lorsqu'une adresse IPv4 privée secondaire est réattribuée à une autre interface, l'adresse IPv4 privée secondaire conserve son association à une adresse IP Elastic.
- Lorsque l'attribution d'une adresse IPv4 privée secondaire est annulée à partir d'une interface, une adresse IP Elastic associée est automatiquement dissociée de l'adresse IPv4 privée secondaire.

Utiliser plusieurs adresses IPv4

Vous pouvez attribuer l'adresse IPv4 privée secondaire à une instance, associer une adresse IPv4 Elastic à l'adresse IPv4 privée secondaire et annuler l'attribution d'une adresse IPv4 privée secondaire.

Tâches

- [Attribuer une adresse IPv4 privée secondaire](#)
- [Configurer le système d'exploitation pour reconnaître les adresses IPv4 privées secondaires](#)
- [Associer une adresse IP Elastic à l'adresse IPv4 privée secondaire](#)
- [Afficher vos adresses IPv4 privées secondaires](#)
- [Annuler l'attribution d'une adresse IPv4 privée secondaire](#)

Attribuer une adresse IPv4 privée secondaire

Vous pouvez attribuer l'adresse IPv4 privée secondaire à l'interface réseau pour une instance au moment du lancement de l'instance ou après celui-ci.

Pour attribuer une adresse IPv4 privée secondaire lors du lancement d'une instance

1. Suivez la procédure pour [lancer une instance](#). Sous [Paramètres réseau](#), choisissez Modifier.
2. Sélectionnez un VPC et un sous-réseau.
3. Développez Configuration réseau avancée.
4. Pour IP secondaire, choisissez Attribuer automatiquement et entrez le nombre d'adresses IP (Amazon attribue automatiquement les adresses IPv4 secondaires) ou choisissez Attribuer manuellement et entrez les adresses IPv4.
5. Complétez les étapes suivantes pour [lancer les instances](#).

Pour attribuer une adresse IPv4 secondaire lors du lancement à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- L'option `--secondary-private-ip-addresses` avec la commande [run-instances](#) (AWS CLI)
- Définissez `-NetworkInterface` et spécifiez le `PrivateIpAddresses` paramètre à l'aide de la [New-EC2Instance](#) commande (AWS Tools for Windows PowerShell).

Pour attribuer une adresse IPv4 privée secondaire à une interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces, puis sélectionnez l'interface réseau pour l'instance.
3. Choisissez Actions, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Sous Adresses IPv4, choisissez Attribuer une nouvelle adresse IP.
5. Entrez une adresse IPv4 spécifique comprise dans la plage de sous-réseau de l'instance, ou laissez le champ vide pour permettre à Amazon de sélectionner une adresse IPv4 pour vous.
6. (Facultatif) Sélectionnez Autoriser pour autoriser la réattribution de l'adresse IP privée secondaire si elle est déjà attribuée à une autre interface réseau.
7. Choisissez Enregistrer.

Vous pouvez également attribuer une adresse IPv4 privée secondaire à une instance. Choisissez Instances dans le panneau de navigation, sélectionnez l'instance et choisissez Actions, sélectionnez Mise en réseau, puis Gérer les adresses IP. Vous pouvez configurer les mêmes informations que précédemment. L'adresse IP est attribuée à l'interface réseau principale (eth0) pour l'instance.

Pour attribuer une adresse IPv4 privée secondaire à une instance existante à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [assign-private-ip-addresses](#) (AWS CLI)
- [Register-EC2PrivateIpAddress](#) (AWS Tools for Windows PowerShell)

Configurer le système d'exploitation pour reconnaître les adresses IPv4 privées secondaires

Une fois que vous avez attribué une adresse IPv4 privée secondaire à votre instance, vous devez configurer le système d'exploitation de cette dernière afin qu'il puisse reconnaître l'adresse IP privée secondaire.

Instances Linux

- Si vous utilisez Amazon Linux, le package `ec2-net-utils` peut effectuer cette opération. Il configure les interfaces réseau supplémentaires associées pendant l'exécution de l'instance, il rafraîchit les adresses IPv4 secondaires au cours du renouvellement du bail DHCP et il met à jour les règles de routage associées. Vous pouvez actualiser immédiatement la liste des interfaces à l'aide de la commande, `sudo service network restart` puis afficher la up-to-date liste à l'aide de `ip addr | i`. Si vous avez besoin d'un contrôle manuel sur votre configuration réseau, vous pouvez supprimer le package `ec2-net-utils`. Pour plus d'informations, consultez [Configurer votre interface réseau à l'aide de ec2-net-utils pour Amazon Linux 2](#).
- Si vous utilisez une autre distribution Linux, consultez la documentation correspondante. Recherchez des informations sur la configuration d'interfaces réseau et d'adresses IPv4 secondaires supplémentaires. Si l'instance a deux ou plusieurs interfaces sur le même sous-réseau, recherchez des informations sur l'utilisation des règles de routage pour contourner le routage asymétrique.

instances Windows

Pour plus d'informations, consultez [Configurer une adresse IPv4 privée secondaire pour votre instance Windows](#).

Associer une adresse IP Elastic à l'adresse IPv4 privée secondaire

Pour associer une adresse IP Elastic à une adresse IPv4 privée secondaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Adresses IP Elastic.
3. Cochez la case correspondant à l'adresse IP élastique
4. Choisissez Actions, puis Associer une adresse IP élastique.
5. Pour Type de ressource, choisissez Interface réseau. Sélectionnez l'interface réseau, puis sélectionnez l'adresse IP secondaire dans la liste des adresses IP privées.

6. Pour Interface réseau, sélectionnez l'interface réseau. Sélectionnez l'adresse IP secondaire dans la liste des adresses IP privées.
7. Pour Adresse IP privée, sélectionnez l'adresse IP secondaire.
8. Choisissez Associer.

Pour associer une adresse IP Elastic à une adresse IPv4 privée secondaire à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [associate-address](#) (AWS CLI)
- [Register-EC2Address](#) (AWS Tools for Windows PowerShell)

Afficher vos adresses IPv4 privées secondaires

Pour consulter les adresses IPv4 privées attribuées à une interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Cochez la case correspondant à l'interface réseau.
4. Dans l'onglet Détails, sous Adresses IP, recherchez l'adresse IPv4 privée et les adresses IPv4 privées secondaires.

Pour consulter les adresses IPv4 privées attribuées à une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Cochez la case correspondant à l'instance.
4. Dans l'onglet Mise en réseau, sous Détails du réseau, recherchez les adresses IPv4 privées et les adresses IPv4 privées secondaires.

Annuler l'attribution d'une adresse IPv4 privée secondaire

Si vous n'avez plus besoin d'une adresse IPv4 privée secondaire, vous pouvez annuler son attribution à partir de l'instance ou de l'interface réseau. Lorsque l'attribution d'une adresse IPv4

privée secondaire est annulée à partir d'une interface réseau, l'adresse IP Elastic (si elle existe) est également dissociée.

Pour annuler l'attribution d'une adresse IPv4 privée secondaire depuis une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez une instance, puis choisissez Actions, Mise en réseau, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Pour les adresses IPv4, choisissez Annuler l'attribution pour l'adresse IPv4 à annuler.
5. Choisissez Enregistrer.

Pour annuler l'attribution d'une adresse IPv4 privée secondaire depuis une interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez l'interface réseau, choisissez Actions, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Pour les adresses IPv4, choisissez Annuler l'attribution pour l'adresse IPv4 à annuler.
5. Choisissez Enregistrer.

Pour annuler l'attribution d'une adresse IPv4 privée secondaire à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [unassign-private-ip-addresses](#) (AWS CLI)
- [Unregister-EC2PrivateIpAddress](#) (AWS Tools for Windows PowerShell)

Utiliser plusieurs adresses IPv6

Vous pouvez attribuer plusieurs adresses IPv6 à votre instance, afficher les adresses IPv6 attribuées à votre instance et annuler l'attribution d'adresses IPv6 à partir de votre instance.

Sommaire

- [Attribuer plusieurs adresses IPv6](#)
- [Afficher vos adresses IPv6](#)
- [Annuler l'attribution d'une adresse IPv6](#)

Attribuer plusieurs adresses IPv6

Vous pouvez attribuer une ou plusieurs adresses IPv6 à votre instance pendant ou après le lancement. Pour attribuer une adresse IPv6 à une instance, le VPC et le sous-réseau dans lequel vous lancez l'instance doivent disposer d'un bloc d'adresses CIDR IPv6 associé.

Pour attribuer plusieurs adresses IPv6 lors du lancement

1. Suivez la procédure pour [lancer une instance](#). Sous [Paramètres réseau](#), choisissez Modifier.
2. Sélectionnez un VPC et un sous-réseau.
3. Développez Configuration réseau avancée.
4. Pour les adresses IP IPv6, choisissez Attribuer automatiquement et le nombre d'adresses IP (Amazon attribue automatiquement les adresses IPv6) ou choisissez Attribuer manuellement et entrez les adresses IPv6.
5. Complétez les étapes suivantes pour [lancer les instances](#).

Vous pouvez utiliser l'écran Instances de la console Amazon EC2 pour attribuer plusieurs adresses IPv6 à une instance existante. Ceci attribue les adresses IPv6 à l'interface réseau principale (eth0) pour l'instance. Pour attribuer une adresse IPv6 spécifique à l'instance, vérifiez que l'adresse IPv6 n'est pas déjà attribuée à une autre instance ou interface réseau.

Pour attribuer plusieurs adresses IPv6 à une instance existante

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez votre instance, choisissez Actions, Mise en réseau, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Pour les adresses IPv6, choisissez Attribuer une nouvelle adresse IP pour chaque adresse IPv6 à ajouter. Vous pouvez spécifier une adresse IPv6 dans la plage du sous-réseau ou laisser le champ vide pour permettre à Amazon de choisir une adresse IPv6 pour vous.
5. Choisissez Enregistrer.

Vous pouvez également attribuer plusieurs adresses IPv6 à une interface réseau existante. L'interface réseau doit avoir été créée dans un sous-réseau qui dispose d'un bloc d'adresses CIDR IPv6 associé. Pour attribuer une adresse IPv6 spécifique à l'interface réseau, vérifiez que l'adresse IPv6 n'est pas déjà affectée à une autre interface réseau.

Pour attribuer plusieurs adresses IPv6 à une interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez votre interface réseau, choisissez Actions, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Pour les adresses IPv6, choisissez Attribuer une nouvelle adresse IP pour chaque adresse IPv6 à ajouter. Vous pouvez spécifier une adresse IPv6 dans la plage du sous-réseau ou laisser le champ vide pour permettre à Amazon de choisir une adresse IPv6 pour vous.
5. Choisissez Enregistrer.

Présentation de la CLI (CLI)

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- Attribuer une adresse IPv6 lors du lancement :
 - Utilisez les options `--ipv6-addresses` ou `--ipv6-address-count` avec la commande [run-instances](#) (AWS CLI)
 - Définissez `-NetworkInterface` et spécifiez les `Ipv6AddressCount` paramètres `Ipv6Addresses` or à l'aide de la [New-EC2Instance](#) commande (AWS Tools for Windows PowerShell).
- Attribuer une adresse IPv6 à une interface réseau :
 - [assign-ipv6-addresses](#) (AWS CLI)
 - `Register-EC2IpvAddressList` (AWS Tools for Windows PowerShell)

Afficher vos adresses IPv6

Vous pouvez afficher les adresses IPv6 d'une instance ou d'une interface réseau.

Pour consulter les adresses IPv6 attribuées à une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Cochez la case correspondant à votre instance.
4. Dans l'onglet Réseau, recherchez le champ Adresses IPv6.

Pour afficher les adresses IPv6 attribuées à une interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Cochez la case correspondant à votre interface réseau.
4. Dans l'onglet Détails, sous Adresses IP, recherchez le champ Adresses IPv6.

Présentation de la CLI (CLI)

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- Afficher les adresses IPv6 d'une instance :
 - [describe-instances](#) (AWS CLI)
 - [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).
- Afficher les adresses IPv6 d'une interface réseau :
 - [describe-network-interfaces](#) (AWS CLI)
 - [Get-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Annuler l'attribution d'une adresse IPv6

Vous pouvez annuler l'attribution d'une adresse IPv6 à partir de l'interface réseau principale d'une instance, ou vous pouvez annuler l'attribution d'une adresse IPv6 à partir d'une interface réseau.

Pour annuler l'attribution d'une adresse IPv6 à partir d'une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.

3. Cochez la case correspondant à votre instance, puis choisissez Actions, Mise en réseau, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Sous Adresses IPv6, choisissez Annuler l'attribution en regard de l'adresse IPv6.
5. Choisissez Enregistrer.

Pour annuler l'attribution d'une adresse IPv6 à partir d'une interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Cochez la case correspondant à votre interface réseau, puis choisissez Actions, Gérer les adresses IP.
4. Sélectionnez l'interface réseau. Sous Adresses IPv6, choisissez Annuler l'attribution en regard de l'adresse IPv6.
5. Choisissez Enregistrer.

Présentation de la CLI (CLI)

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [unassign-ipv6-addresses](#) (AWS CLI)
- `Unregister-EC2Ipv6AddressList` (AWS Tools for Windows PowerShell)

Configurer une adresse IPv4 privée secondaire pour votre instance Windows

Vous pouvez spécifier plusieurs adresses IPv4 privées pour vos instances. Une fois que vous avez attribué une adresse IPv4 privée secondaire à une instance, vous devez configurer le système d'exploitation de cette dernière afin qu'il puisse reconnaître l'adresse IPv4 privée secondaire.

Note

Ces instructions sont basées sur Windows Server 2022. La mise en œuvre de ces étapes peut varier en fonction du système d'exploitation de l'instance Windows.

Tâches

- [Prérequis](#)
- [Étape 1 : configurer l'adressage IP statique dans votre instance](#)
- [Étape 2 : Configurer une adresse IP privée secondaire pour votre instance](#)
- [Étape 3 : Configurer les applications pour qu'elles utilisent l'adresse IP privée secondaire](#)

Prérequis

1. Attribuez l'adresse IPv4 privée secondaire à l'interface réseau pour l'instance. Vous pouvez attribuer l'adresse IPv4 privée secondaire lors que vous lancez l'instance ou une fois celle-ci en cours d'exécution. Pour plus d'informations, consultez [Attribuer une adresse IPv4 privée secondaire](#).
2. Allouez une adresse IP Elastic et associez-la à l'adresse IPv4 privée secondaire. Pour plus d'informations, consultez [allouer une adresse IP Elastic](#) ; et [Associer une adresse IP Elastic à l'adresse IPv4 privée secondaire](#).

Étape 1 : configurer l'adressage IP statique dans votre instance

Pour activer votre instance Windows afin d'utiliser plusieurs adresses IP, vous devez configurer votre instance pour utiliser l'adressage IP statique plutôt qu'un serveur DHCP.

Important

Lorsque vous configurez l'adressage IP statique dans votre instance, l'adresse IP doit correspondre exactement à ce qui est affiché dans la console, la CLI ou l'API. Si vous entrez ces adresses IP de manière incorrecte, l'instance peut devenir inaccessible.

Pour configurer l'adressage IP statique sur une instance Windows

1. Connectez-vous à votre instance.
2. Recherchez l'adresse IP, le masque de sous-réseau et les adresses de passerelle par défaut pour l'instance en exécutant les étapes suivantes :
 - Exécutez la commande suivante dans PowerShell :

```
ipconfig /all
```

Passez en revue le résultat et notez les valeurs de l'adresse IPv4, du masque de sous-réseau, de la passerelle par défaut et des serveurs DNS pour l'interface réseau. Votre sortie doit ressembler à l'exemple suivant :

```
...

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . : us-west-2.compute.internal
    Description . . . . . : Amazon Elastic Network Adapter #2
    Physical Address. . . . . : 02-9C-3B-FC-8E-67
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
    IPv4 Address. . . . . : 10.200.0.128(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Monday, April 8, 2024 12:19:29 PM
    Lease Expires . . . . . : Monday, April 8, 2024 4:49:30 PM
    Default Gateway . . . . . : 10.200.0.1
    DHCP Server . . . . . : 10.200.0.1
    DHCPv6 IAID . . . . . : 151166011
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
E7
    DNS Servers . . . . . : 10.200.0.2
    NetBIOS over Tcpip. . . . . : Enabled
```

3. Ouvrez le Centre de réseau et de partage en exécutant la commande suivante dans PowerShell :

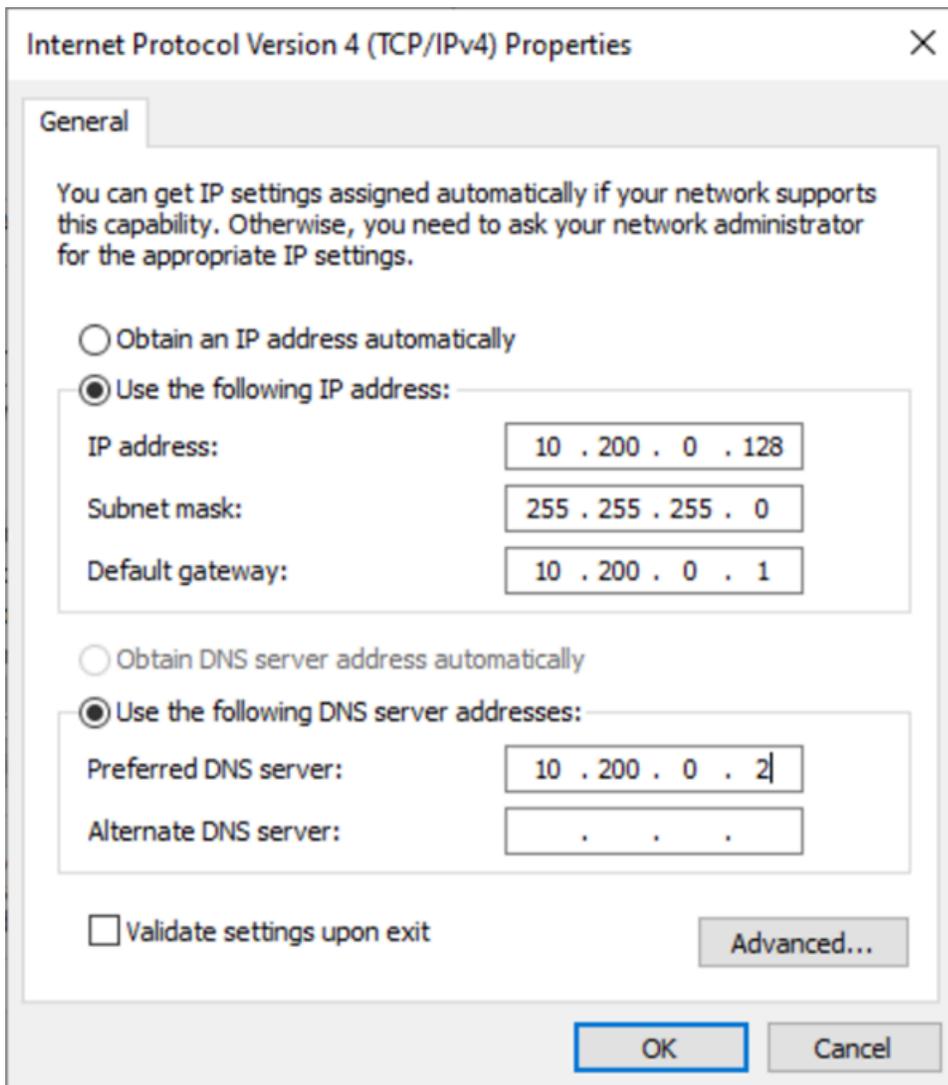
```
& $env:SystemRoot\system32\control.exe ncpa.cpl
```

4. Ouvrez le menu contextuel (clic droit) de l'interface réseau (connexion au réseau local ou Ethernet) et choisissez Propriétés.
5. Choisissez Protocole Internet version 4 (TCP/IPv4), puis Propriétés.
6. Dans la boîte de dialogue Propriétés du Protocole Internet version 4 (TCP/IPv4), choisissez Utiliser l'adresse IP suivante, entrez les valeurs suivantes, puis choisissez OK.

Champ	Value
Adresse IP	Adresse IPv4 obtenue à l'étape 2 ci-dessus.
Masque de sous-réseau	Masque de sous-réseau obtenu à l'étape 2 ci-dessus.
Passerelle par défaut	Passerelle par défaut obtenue à l'étape 2 ci-dessus.
Serveur DNS préféré	Serveur DNS obtenu à l'étape 2 ci-dessus.
Serveur DNS auxiliaire	Serveur DNS auxiliaire obtenu à l'étape 2 ci-dessus. Si aucun serveur DNS auxiliaire n'a été répertorié, laissez ce champ vide.

 Important

Si vous définissez l'adresse IP sur n'importe quelle valeur autre que l'adresse IP actuelle, vous perdrez la connectivité à l'instance.



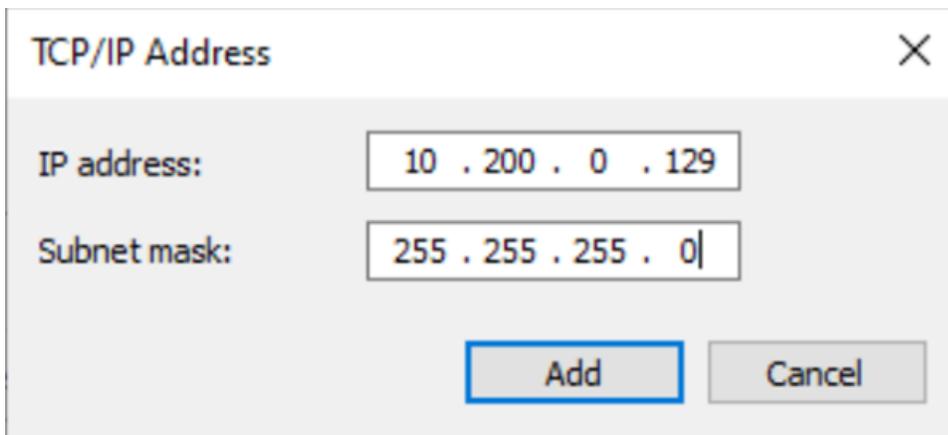
Vous perdrez la connectivité RDP à l'instance Windows pendant quelques secondes pendant que l'instance passe de l'utilisation du DHCP à celle de l'adressage statique. L'instance conserve les mêmes informations d'adresse IP qu'auparavant, mais ces informations sont désormais statiques et ne sont plus opérées par le DHCP.

Étape 2 : Configurer une adresse IP privée secondaire pour votre instance

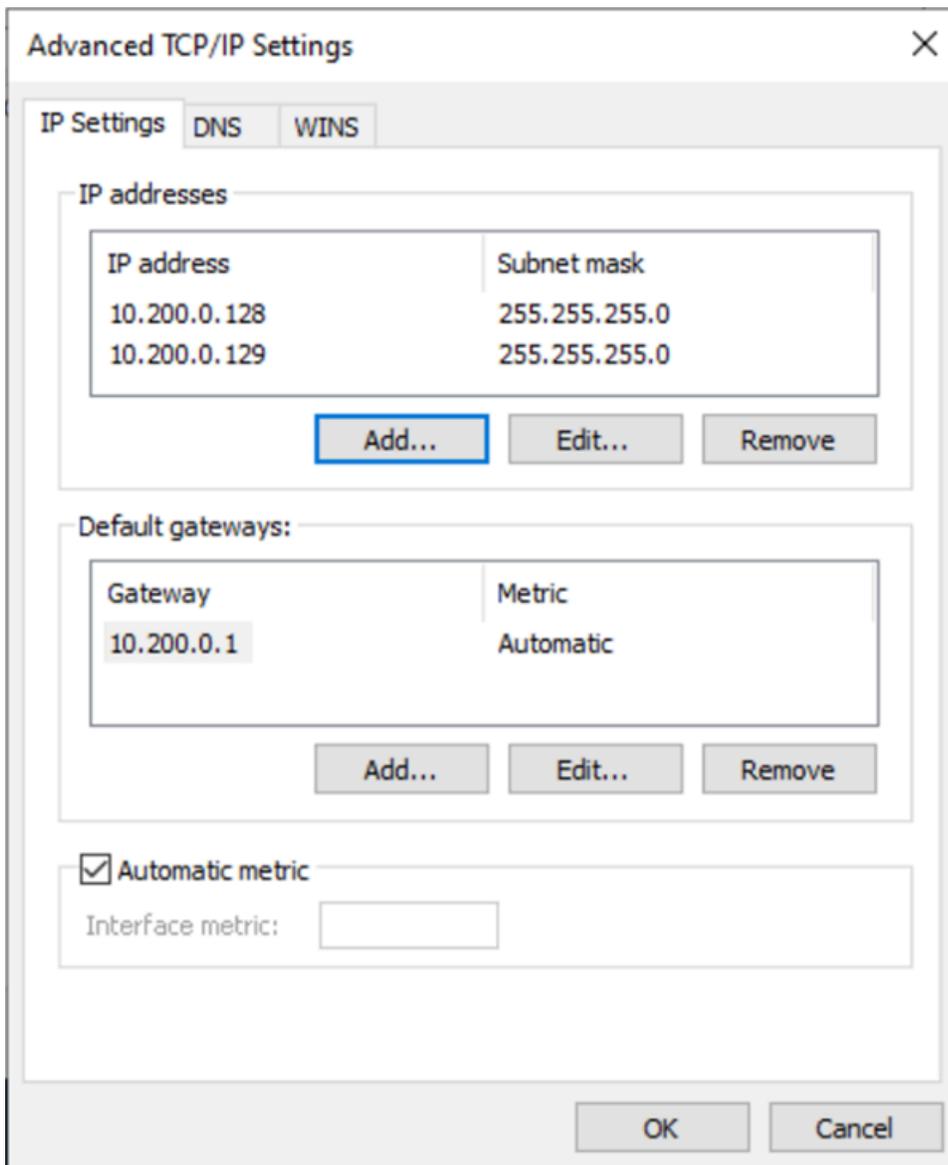
Après avoir configuré l'adressage IP statique sur votre instance Windows, vous pouvez préparer une seconde adresse IP privée.

Pour configurer une adresse IP secondaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Instances, puis choisissez votre instance.
3. Notez l'adresse IP secondaire que vous trouverez sur la page Mise en réseau.
4. Connectez-vous à votre instance.
5. Sur votre instance Windows, choisissez Démarrer, Panneau de configuration.
6. Choisissez Réseau et Internet, Centre Réseau et partage.
7. Sélectionnez l'interface réseau (connexion au réseau local ou Ethernet) et choisissez Propriétés.
8. Sur la page Propriétés de la Connexion au réseau local, choisissez Protocole Internet version 4 (TCP/IPv4), Propriétés, Avancées.
9. Choisissez Add (Ajouter).
10. Dans la boîte de dialogue Adresse TCP/IP, saisissez l'adresse IP privée secondaire dans Adresse IP. Dans Masque de sous-réseau, saisissez le même masque de sous-réseau que celui que vous avez entré pour l'adresse IP privée principale dans [Étape 1 : configurer l'adressage IP statique dans votre instance](#), puis choisissez Ajouter.



11. Vérifiez les paramètres de l'adresse IP et choisissez OK.



12. Choisissez OK, Fermer.
13. Pour vérifier que l'adresse IP secondaire a été ajoutée au système d'exploitation, exécutez la `ipconfig /all` commande dans PowerShell. Votre sortie doit ressembler à ce qui suit :

Ethernet adapter Ethernet 4:

```

Connection-specific DNS Suffix . :
Description . . . . . : Amazon Elastic Network Adapter #2
Physical Address. . . . . : 02-9C-3B-FC-8E-67
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
IPv4 Address. . . . . : 10.200.0.128(Preferred)

```

```
Subnet Mask . . . . . : 255.255.255.0
IPv4 Address. . . . . : 10.200.0.129(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.200.0.1
DHCPv6 IAID . . . . . : 151166011
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
DNS Servers . . . . . : 10.200.0.2
NetBIOS over Tcpi. . . . . : Enabled
```

Étape 3 : Configurer les applications pour qu'elles utilisent l'adresse IP privée secondaire

Vous pouvez configurer toutes les applications pour qu'elles utilisent l'adresse IP privée secondaire. Par exemple, si votre instance s'exécute sur un site web sur IIS, vous pouvez configurer IIS pour qu'il utilise l'adresse IP privée secondaire.

Pour configurer IIS pour qu'il utilise l'adresse IP privée secondaire

1. Connectez-vous à votre instance.
2. Ouvrez le gestionnaire d'Internet Information Services (IIS).
3. Dans le volet Connexions, développez Sites.
4. Ouvrez le menu contextuel (clic droit) de votre site web et choisissez Modifier les liaisons.
5. Dans la boîte de dialogue Liaisons de site, pour Type, choisissez http, Modifier.
6. Dans la boîte de dialogue Modifier une liaison de site, pour Adresse IP, sélectionnez l'adresse IP privée secondaire. (Par défaut, chaque site web accepte les demandes HTTP de toutes les adresses IP.)

The screenshot shows the 'Edit Site Binding' dialog box. It has three main input fields: 'Type' (a dropdown menu set to 'http'), 'IP address' (a text box containing '10.200.0.129'), and 'Port' (a text box containing '80'). Below these is a 'Host name' field with a dropdown menu. The dropdown menu is open, showing three options: 'All Unassigned', '10.200.0.129', and '10.200.0.128'. Below the dropdown is an example: 'Example: www.contoso.com or marketing.contoso.com'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

7. Choisissez OK, Fermer.

Noms d'hôtes d'instance EC2

Lorsque vous créez une instance EC2, AWS crée un nom d'hôte pour cette instance. Pour plus d'informations sur les types de noms d'hôtes et sur la manière dont ils sont fournis AWS, consultez [Types de noms d'hôtes des instances Amazon EC2](#). Amazon fournit un serveur DNS qui résout les noms d'hôtes fournis par Amazon en adresses IPv4 et IPv6. Le serveur Amazon DNS se trouve à la base de votre plage réseau VPC plus deux. Pour plus d'informations, consultez [DNS attributes for your VPC](#) (Attributs DNS pour votre VPC) dans le Guide de l'utilisateur d'Amazon VPC.

Adresses lien-local

Les adresses lien-local sont des adresses IP connues et non routables. Amazon EC2 utilise les adresses de l'espace d'adressage lien-local pour fournir des services accessibles uniquement depuis une instance EC2. Ces services ne s'exécutent pas sur l'instance, ils s'exécutent sur l'hôte sous-jacent. Lorsque vous accédez aux adresses lien-local pour ces services, vous communiquez soit avec l'hyperviseur Xen, soit avec le contrôleur Nitro.

Plage d'adresses lien-local

- IPv4 – 169.254.0.0/16 (169.254.0.0 à 169.254.255.255)
- IPv6 – fe80::/10

Services auxquels vous accédez à l'aide d'adresses lien-local

- [Service des métadonnées d'instance](#)
- [Amazon Route 53 Resolver](#) (également connu sous le nom de serveur DNS Amazon)
- [Service de synchronisation temporelle d'Amazon](#)

Types de noms d'hôtes des instances Amazon EC2

Cette section décrit les types de noms d'hôte de systèmes d'exploitation invités des instances Amazon EC2 disponibles lorsque vous lancez des instances dans vos sous-réseaux VPC.

Le nom d'hôte distingue les instances EC2 de votre réseau. Vous pouvez utiliser le nom d'hôte d'une instance si, par exemple, vous souhaitez exécuter des scripts pour communiquer avec toutes ou certaines instances de votre réseau.

Table des matières

- [Types de noms d'hôte EC2](#)
- [Où vous voyez le nom de la ressource et le nom d'adresse IP](#)
- [Comment décider s'il faut choisir le nom de la ressource ou le nom IP](#)
- [Modifier le type de nom d'hôte et les configurations de noms d'hôte DNS](#)

Types de noms d'hôte EC2

Il existe deux types de noms d'hôte pour le nom d'hôte du système d'exploitation invité lorsque des instances EC2 sont lancées dans un VPC :

- Nom de l'adresse IP : schéma de noms hérité dans lequel, lorsque vous lancez une instance, l'adresse IPv4 privée de l'instance est incluse dans le nom d'hôte de l'instance. Le nom de l'adresse IP existe pour toute la durée de vie de l'instance EC2. Lorsqu'il est utilisé comme nom d'hôte DNS privé, il renvoie uniquement l'adresse IPv4 privée (enregistrement A).

- **Nom des ressources** : lorsque vous lancez une instance, l'ID d'instance EC2 est inclus dans le nom d'hôte de l'instance. Le nom des ressources existe pour la durée de vie de l'instance EC2. Lorsqu'il est utilisé comme nom d'hôte DNS privé, il peut renvoyer à la fois l'adresse IPv4 privée (enregistrement A) ou à l'adresse IPv6 Global Unicast (enregistrement AAAA).

Le type de nom d'hôte du système d'exploitation invité de l'instance EC2 dépend des paramètres du sous-réseau :

- Si l'instance est lancée dans un sous-réseau exclusivement IPv4, vous pouvez sélectionner le nom d'adresse IP ou le nom des ressources.
- Si l'instance est lancée dans un sous-réseau à double pile (IPv4 + IPv6), vous pouvez sélectionner un nom d'adresse IP ou le nom des ressources.
- Si l'instance est lancée dans un sous-réseau exclusivement IPv6, le nom des ressources est utilisé automatiquement.

Table des matières

- [Nom d'adresse IP](#)
- [Nom de la ressource](#)
- [La différence entre le nom d'adresse IP et le nom de la ressource](#)

Nom d'adresse IP

Lorsque vous lancez une instance EC2 avec le Hostname type (Type de nom d'hôte) de l'IP name (Nom de l'adresse IP), le nom d'hôte du système d'exploitation invité est configuré pour utiliser l'adresse IPv4 privée.

- Format d'une instance dans us-east-1 : `private-ipv4-address.ec2.internal`
- Exemple : `ip-10-24-34-0.ec2.internal`
- Format pour une instance dans n'importe quelle autre AWS région : `private-ipv4-address.region.compute.internal`
- Exemple : `ip-10-24-34-0.us-west-2.compute.internal`

Nom de la ressource

Lorsque vous lancez des instances EC2 dans des sous-réseaux uniquement IPv6, le Hostname type (Type de nom d'hôte) de Resource name (Nom de la ressource) est sélectionné par défaut. Lorsque vous lancez une instance dans des sous-réseaux IPv4 uniquement ou à double pile (IPv4 + IPv6), le Nom de la ressource est une option que vous pouvez sélectionner. Après avoir lancé une instance, vous pouvez gérer la configuration du nom d'hôte. Pour plus d'informations, consultez [Modifier le type de nom d'hôte et les configurations de noms d'hôte DNS](#).

Lorsque vous lancez une instance EC2 avec un Hostname type (Type de nom d'hôte) de Resource name (Nom des ressources), le nom d'hôte du système d'exploitation invité est configuré pour utiliser l'ID de l'instance EC2.

- Format d'une instance dans us-east-1 : `ec2-instance-id.ec2.internal`
- Exemple : `i-0123456789abcdef.ec2.internal`
- Format pour une instance dans n'importe quelle autre AWS région : `ec2-instance-id.region.compute.internal`
- Exemple : `i-0123456789abcdef.us-west-2.compute.internal`

La différence entre le nom d'adresse IP et le nom de la ressource

Les requêtes DNS pour les noms d'adresse IP et les noms des ressources coexistent afin de garantir la rétrocompatibilité et de vous permettre de migrer de la dénomination basée sur les adresses IP pour les noms d'hôtes vers la dénomination basée sur les ressources. Pour les noms d'hôtes DNS privés basés sur les noms d'adresses IP, vous ne pouvez pas configurer si une requête d'enregistrement A DNS pour l'instance reçoit une réponse ou non. Les requêtes d'enregistrement A du DNS sont toujours résolues, quels que soient les paramètres du nom d'hôte du système d'exploitation invité. En revanche, pour les noms d'hôtes DNS privés basés sur le nom de ressources, vous pouvez configurer si les requêtes DNS A ou DNS AAAA de l'instance reçoivent une réponse ou non. Vous configurez le comportement de réponse lorsque vous lancez une instance ou modifiez un sous-réseau. Pour plus d'informations, consultez [Modifier le type de nom d'hôte et les configurations de noms d'hôte DNS](#).

Où vous voyez le nom de la ressource et le nom d'adresse IP

Cette section décrit où vous pouvez consulter les types de nom d'hôte, nom de ressource et d'adresse IP dans la console EC2.

Table des matières

- [Lors de la création d'une instance EC2](#)
- [Lors de la consultation des détails d'une instance EC2 existante](#)

Lors de la création d'une instance EC2

Lorsque vous créez une instance EC2, selon le type de sous-réseau que vous sélectionnez, le Hostname type (Type de nom d'hôte) de Resource name (Nom de la ressource) peut être disponible, ou il peut être sélectionné et non modifiable. Cette section décrit les scénarios dans lesquels vous pouvez consulter les types de nom d'hôte, nom de ressource et d'adresse IP.

Scénario 1

Vous créez une instance EC2 dans l'assistant (voir [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#)) et, lorsque vous configurez les détails, vous choisissez un sous-réseau que vous avez configuré pour être exclusivement IPv6.

Dans ce cas, le champ Hostname type (Type de nom d'hôte) de Resource name (Nom de la ressource) est sélectionné automatiquement et n'est pas modifiable. Les options DNS Hostname (Nom d'hôte DNS) de Enable IP name IPV4 (A record) DNS requests (Activer les requêtes DNS IPV4 (enregistrement A) de nom IP) et Enable resource-based IPV4 (A record) DNS requests (Activer les requêtes DNS IPV4 (enregistrement A) basées sur les ressources) sont désélectionnés automatiquement et ne sont pas modifiables. Enable resource-based IPv6 (AAAA record) DNS requests (Activer les requêtes DNS IPV6 (enregistrement AAAA) basées sur les ressources) est sélectionné par défaut, mais est modifiable. Si cette option est sélectionnée, les requêtes DNS portant sur le nom de la ressource seront résolues à l'adresse IPv6 (enregistrement AAAA) de cette instance EC2.

Scénario 2

Vous créez une instance EC2 dans l'assistant (voir [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#)) et, lorsque vous configurez les détails, vous choisissez un sous-réseau configuré avec un bloc d'adresse CIDR IPv4 ou un bloc d'adresse CIDR IPv4 et IPv6 (« double pile »).

Dans ce cas, Enable IP name IPV4 (A record) DNS requests (Activer les requêtes DNS IPV4 (enregistrement A) de nom IP) est sélectionné automatiquement et ne peut pas être modifié. Cela signifie que les requêtes au nom IP seront résolues à l'adresse IPv4 (enregistrement A) de cette instance EC2.

Les options correspondent par défaut aux configurations du sous-réseau, mais vous pouvez modifier les options de cette instance en fonction des paramètres du sous-réseau :

- **Hostname type (Type de nom d'hôte)** : détermine si vous souhaitez que le nom d'hôte du système d'exploitation invité de l'instance EC2 soit le nom de ressource ou le nom IP. La valeur par défaut est IP name (Nom d'adresse IP).
- **Enable resource-based IPv4 (A record) DNS requests (Activer les requêtes DNS IPv4 (enregistrement A) basées sur les ressources)** : détermine si les demandes adressées au nom de votre ressource sont résolues vers l'adresse IPv4 privée (enregistrement A) de cette instance EC2. Cette option n'est pas sélectionnée par défaut.
- **Enable resource-based IPv6 (AAAA record) DNS requests (Activer les requêtes DNS IPv6 (enregistrement AAAA) basées sur les ressources)** : détermine si les demandes adressées au nom de votre ressource sont résolues vers l'adresse IPv6 privée (enregistrement AAAA) de cette instance EC2. Cette option n'est pas sélectionnée par défaut.

Lors de la consultation des détails d'une instance EC2 existante

Vous pouvez voir les valeurs du nom d'hôte d'une instance EC2 existante dans l'onglet Details (Détails) de l'instance EC2 :

- **Hostname type (Type de nom d'hôte)** : nom d'hôte au format nom IP ou nom de ressource.
- **Private IP DNS name (IPv4 only) (Nom de DNS IP privé (exclusivement IPv4))** : nom IP qui sera toujours résolu à l'adresse IPv4 privée de l'instance.
- **Private resource DNS name (Nom de DNS de la ressource privée)** : nom de ressource qui se résout aux enregistrements DNS sélectionnés pour cette instance.
- **Answer private resource DNS name (Réponse ressource privée Nom DNS)** : le nom de ressource se résout en enregistrements DNS IPv4 (A), IPv6 (AAAA) ou IPv4 et IPv6 (A et AAAA).

De plus, si vous vous connectez à votre instance EC2 directement via SSH et que vous saisissez la commande `hostname`, vous verrez le nom d'hôte au format du nom IP ou du nom de ressource.

Comment décider s'il faut choisir le nom de la ressource ou le nom IP

Lorsque vous lancez une instance EC2 (voir [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#)), si vous choisissez un Hostname Type (Type de nom d'hôte) de Resource name (Nom de la ressource), l'instance EC2 se lance avec un nom d'hôte au format de nom de

ressource. Dans ce cas, l'enregistrement DNS de cette instance EC2 peut également pointer vers le nom de la ressource. Cela vous permet de choisir si ce nom d'hôte correspond à l'adresse IPv4, à l'adresse IPv6 ou à la fois aux adresses IPv4 et IPv6 de l'instance. Si vous envisagez d'utiliser IPv6 à l'avenir ou si vous utilisez des sous-réseaux à double pile aujourd'hui, il est préférable d'utiliser un Hostname type (Type de nom d'hôte) de Resource name (Nom de la ressource) afin de modifier la résolution DNS des noms d'hôtes de vos instances sans modifier les enregistrements DNS eux-mêmes. Le nom de la ressource vous permet d'ajouter et de supprimer une résolution DNS IPv4 et IPv6 sur une instance EC2.

Si, à la place, vous choisissez un Hostname type (Type de nom d'hôte) de IP name (Nom d'adresse IP), et l'utilisez comme nom d'hôte DNS, il peut uniquement être résolu à l'adresse IPv4 de l'instance. Il ne se résoudra pas à l'adresse IPv6 de l'instance même si l'instance possède à la fois une adresse IPv4 et une adresse IPv6 associées.

Modifier le type de nom d'hôte et les configurations de noms d'hôte DNS

Suivez les étapes de cette section pour modifier les configurations de type de nom d'hôte et de nom d'hôte DNS pour les sous-réseaux ou les instances EC2 après leur lancement.

Table des matières

- [Sous-réseaux](#)
- [Instances EC2](#)

Sous-réseaux

Modifiez les configurations d'un sous-réseau en sélectionnant un sous-réseau dans la console VPC et en choisissant Actions, Edit subnet settings (Modifier les paramètres du sous-réseau).

Note

La modification des paramètres du sous-réseau ne modifie pas la configuration des instances EC2 déjà lancées dans le sous-réseau.

- Hostname type (Type de nom d'hôte) : détermine si vous souhaitez que le paramètre par défaut du nom d'hôte du système d'exploitation invité de l'instance EC2 lancée dans le sous-réseau soit le nom de ressource ou le nom IP.

- Enable DNS hostname IPv4 (A record) requests [Activer les demandes IPv4 (enregistrement A) de nom d'hôte DNS] : détermine si les demandes/requêtes DNS portant sur le nom de votre ressource sont résolues vers l'adresse IPv4 privée (enregistrement A) de cette instance EC2.
- Enable DNS hostname IPv6 (AAAA record) requests (Activer les demandes IPv6 (enregistrement A) de nom d'hôte DNS) : détermine si les demandes/requêtes DNS portant sur le nom de votre ressource sont résolues vers l'adresse IPv6 (enregistrement AAAA) de cette instance EC2.

Instances EC2

Suivez les étapes de cette section pour modifier les configurations de type de nom d'hôte et de nom d'hôte DNS d'une instance EC2.

Important

- Pour modifier le paramètre Use resource based naming as guest OS hostname (Utiliser la dénomination basée sur les ressources comme nom d'hôte du système d'exploitation invité), vous devez d'abord arrêter l'instance. Pour modifier le paramètre Réponse à la demande de nom d'hôte DNS IPv4 (enregistrement A) ou Réponse aux demandes de nom d'hôte DNS IPv6 (enregistrement AAAA), il n'est pas nécessaire d'arrêter l'instance.
- Pour modifier les paramètres des types d'instance EC2 non basés sur EBS, vous ne pouvez pas arrêter l'instance. Vous devez résilier l'instance et en lancer une nouvelle avec les configurations de type de nom d'hôte et de nom d'hôte DNS souhaitées.

Pour modifier les configurations de type de nom d'hôte et de nom d'hôte DNS pour une instance EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Si vous avez l'intention de modifier le paramètre Use resource based naming as guest OS hostname (Utiliser la dénomination basée sur les ressources comme nom d'hôte du système d'exploitation invité), arrêtez d'abord l'instance EC2. Sinon, ignorez cette étape.

Pour arrêter l'instance, sélectionnez l'instance et choisissez Instance state (État de l'instance), Stop instance (Arrêter l'instance).

3. Sélectionnez l'instance, puis choisissez Actions, Instance settings (Paramètres des instances), Change resource based naming options (Modifier les options de dénomination basées sur les ressources).

- Use resource based naming as guest OS hostname (Utiliser la dénomination basée sur les ressources comme nom d'hôte du système d'exploitation invité) : détermine si vous souhaitez que le nom d'hôte du système d'exploitation invité de l'instance EC2 soit le nom de ressource ou le nom IP.
 - Answer DNS hostname IPv4 (A record) request [Réponse aux demandes de nom d'hôte DNS IPv4 (enregistrement A)] : détermine si les requêtes/demandes DNS à votre nom de ressource se résolvent à l'adresse IPv4 privée de cette instance EC2.
 - Answer DNS hostname IPv6 (AAAA record) requests (Réponse aux demandes de nom d'hôte DNS IPv6 (enregistrement AAAA)) : détermine si les requêtes/demandes DNS vers votre nom de ressource se résolvent à l'adresse IPv6 (enregistrement AAAA) de cette instance EC2.
4. Choisissez Enregistrer.
 5. Si vous aviez arrêté l'instance, redémarrez-la.

Fourniture de vos propres adresses IP (BYOIP) dans Amazon EC2

Vous pouvez transférer une partie ou la totalité de votre plage d'adresses IPv4 ou IPv6 routables publiquement de votre réseau local vers votre compte. AWS Vous continuez à contrôler la plage d'adresses et vous pouvez en faire la publicité sur Internet via AWS. Une fois que vous avez transféré la plage d'adresses AWS, elle apparaît dans votre AWS compte sous forme de pool d'adresses.

Pour obtenir la liste des régions où BYOIP est disponible, consultez [Disponibilité par région](#).

Note

- Les étapes de cette page décrivent comment fournir votre propre plage d'adresses IP pour l'utiliser dans Amazon EC2 uniquement.
- Pour apporter votre propre plage d'adresses IP à utiliser AWS Global Accelerator, consultez la section [Apporter vos propres adresses IP \(BYOIP\)](#) dans le guide du AWS Global Accelerator développeur.
- Pour apporter votre propre plage d'adresses IP à utiliser Amazon VPC IP Address Manager, consultez le [didacticiel : Transférer vos adresses IP à l'IPAM](#) dans le guide de l'utilisateur Amazon VPC IPAM.

Table des matières

- [Définitions BYOIP](#)
- [Exigences et quotas](#)
- [Conditions préalables à l'onboarding de votre plage d'adresses BYOIP](#)
- [Intégrer votre BYOIP](#)
- [Utiliser votre plage d'adresses](#)
- [Valider votre BYOIP](#)
- [Disponibilité par région](#)
- [Disponibilité de la zone locale](#)
- [En savoir plus](#)

Définitions BYOIP

- Certificat auto-signé X.509 : norme de certificat la plus couramment utilisée pour chiffrer et authentifier les données au sein d'un réseau. Il s'agit d'un certificat utilisé AWS pour valider le contrôle de l'espace IP à partir d'un enregistrement RDAP. Pour plus d'informations sur les certificats X.509, consultez [RFC 3280](#).
- Numéro de système autonome (ASN) : identifiant unique au monde qui définit un groupe de préfixes IP gérés par un ou plusieurs opérateurs réseau qui appliquent une politique de routage unique et clairement définie.
- Registre Internet régional (RIR) : organisation qui gère l'attribution et l'enregistrement des adresses IP et des ASN dans une région du monde.
- Protocole d'accès aux données de registre (RDAP) : protocole en lecture seule permettant d'interroger les données d'enregistrement actuelles dans un RIR. Les entrées de la base de données RIR interrogée sont appelées « enregistrements RDAP ». Certains types d'enregistrements doivent être mis à jour par les clients via un mécanisme fourni par le RIR. Ces enregistrements sont interrogés AWS pour vérifier le contrôle d'un espace d'adressage dans le RIR.
- Autorisation d'origine d'itinéraire (ROA) : objet créé par les RIR pour que les clients authentifient la publicité IP, en particulier les systèmes autonomes. Pour obtenir une présentation, consultez [Autorisation d'origine d'itinéraire \(ROA\)](#) sur le site web d'ARIN.
- Registre Internet local (LIR) : organisations telles que les fournisseurs de services Internet qui allouent un bloc d'adresses IP à partir d'un RIR à leurs clients.

Exigences et quotas

- La plage d'adresses doit être enregistrée dans votre registre Internet régional (RIR). Consultez votre RIR pour connaître les politiques relatives aux régions géographiques. BYOIP prend actuellement en charge l'enregistrement dans l'ARIN (American Registry for Internet Numbers), le RIPE (Réseaux IP Européens Network Coordination Centre) ou l'APNIC (Asia-Pacific Network Information Centre). Elle doit être enregistrée pour une entreprise ou une entité institutionnelle et ne peut pas être enregistrée pour une personne individuelle.
- La plage d'adresses IPv4 la plus spécifique que vous pouvez apporter est /24.
- [La plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR pouvant faire l'objet d'une publicité publique et /56 pour les CIDR qui ne le sont pas.](#)
- Les ROA ne sont pas nécessaires pour les plages CIDR qui ne sont pas publiquement publiées, mais les registres RDAP doivent toujours être mis à jour.
- Vous pouvez attribuer chaque plage d'adresses à une AWS région à la fois.
- Vous pouvez ajouter à votre compte un total de cinq plages d'adresses BYOIP IPv4 et IPv6 par AWS région. AWS Vous ne pouvez pas ajuster les quotas pour les CIDR BYOIP à l'aide de la console Service Quotas, mais vous pouvez demander une augmentation des quotas en contactant le AWS Support Center comme décrit dans la section [Quotas de AWS service](#) du. Références générales AWS
- Vous ne pouvez pas partager votre plage d'adresses IP avec d'autres comptes, AWS RAM sauf si vous utilisez Amazon VPC IP Address Manager (IPAM) et si vous intégrez IPAM à Organizations. AWS Pour plus d'informations, consultez [Intégrer l'IPAM aux AWS organisations](#) dans le guide de l'utilisateur Amazon VPC IPAM.
- L'historique des adresses de la plage d'adresses IP doit être propre. Nous pouvons enquêter sur la réputation de la plage d'adresses IP et nous réserver le droit de rejeter une plage d'adresses IP si elle contient une adresse IP qui a une mauvaise réputation ou qui est associée à un comportement malveillant.
- L'espace d'adressage hérité IPv4 qui était distribué par le registre central de l'IANA (Internet Assigned Numbers Authority) avant la création du système de registre Internet régional (RIR), nécessite toujours un objet ROA correspondant.
- Il est courant que les LIR utilisent un processus manuel pour mettre à jour leurs registres. Ce déploiement peut prendre plusieurs jours en fonction de la LIR.

- Un seul objet ROA et un registre RDAP sont nécessaires pour un bloc d'adresse CIDR volumineux. Vous pouvez transférer plusieurs blocs CIDR plus petits de cette plage AWS, même dans plusieurs AWS régions, en utilisant un seul objet et un seul enregistrement.
- Le BYOIP n'est pas pris en charge pour Wavelength Zones ou versions ultérieures. AWS Outposts
- N'apportez aucune modification manuelle à BYOIP dans RADb ou dans tout autre IRR. BYOIP mettra automatiquement à jour RADb. Toute modification manuelle incluant l'ASN de BYOIP entraînera l'échec de l'opération de mise à disposition de BYOIP.
- Une fois que vous avez transféré une plage d'adresses IPv4 AWS, vous pouvez utiliser toutes les adresses IP de la plage, y compris la première adresse (adresse réseau) et la dernière adresse (adresse de diffusion).

Conditions préalables à l'onboarding de votre plage d'adresses BYOIP

Le processus d'onboarding de BYOIP comporte deux phases, pour lesquelles vous devez effectuer trois étapes. Ces étapes correspondent aux étapes décrites dans le diagramme suivant. Nous incluons des étapes manuelles dans cette documentation, mais votre RIR peut proposer des services gérés pour vous aider au cours de ces étapes.

Phase de préparation

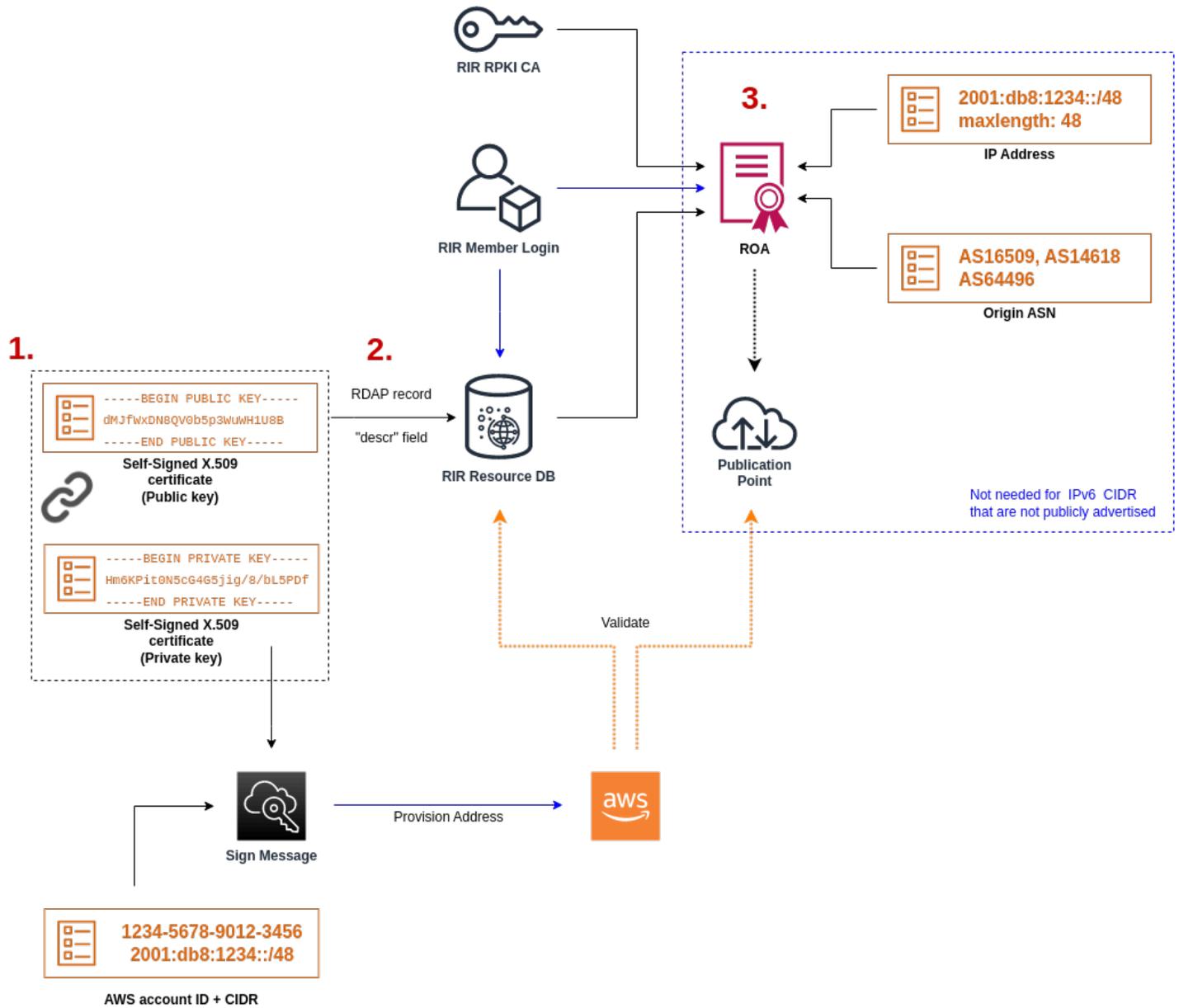
1. [Créez une paire de clés RSA](#) et utilisez-la pour générer un certificat X.509 auto-signé à des fins d'authentification. Ce certificat n'est utilisé que pendant la phase d'allocation.

Phase de configuration RIR

2. [Chargez le certificat auto-signé](#) dans vos commentaires de registre RDAP.
3. [Créez un objet ROA dans votre RIR](#). Le ROA définit la plage d'adresses souhaitée, les numéros système autonomes (ASN) autorisés à publier la plage d'adresses et une date d'expiration à enregistrer avec l'infrastructure RPKI (Resource Public Key Infrastructure) de votre RIR.

Note

Un ROA n'est pas nécessaire pour les espaces d'adressage IPv6 qui ne sont pas publiquement publiés.



Pour ajouter plusieurs plages d'adresses non-contiguës, vous devez répéter ce processus avec chacune d'elles. Cependant, il n'est pas nécessaire de répéter les étapes de préparation et de configuration du RIR si vous divisez un bloc contigu sur plusieurs régions différentes. AWS

L'ajout d'une plage d'adresses n'a aucun effet sur les plages d'adresses que vous avez ajoutées précédemment.

⚠ Important

Avant d'intégrer votre plage d'adresses, respectez les prérequis suivants. Les tâches de cette section nécessitent un terminal Linux et peuvent être effectuées à l'aide de Linux, du [AWS CloudShell](#) ou du [sous-système Windows pour Linux](#).

1. Création d'une clé privée et génération d'un certificat X.509

Utilisez la procédure suivante pour créer un certificat X509 auto-signé et l'ajouter au registre RDAP de votre RIR. Cette paire de clés est utilisée pour authentifier la plage d'adresses auprès du RIR. Les commandes openssl exigent OpenSSL version 1.0.2 ou ultérieure.

Copiez les commandes suivantes et remplacez uniquement les valeurs d'espace réservé (en italique et en couleur).

Cette procédure suit la bonne pratique consistant à chiffrer votre clé RSA privée et à exiger une phrase secrète pour y accéder.

1. Générez une paire de clés RSA 2048 bits comme indiqué ci-après.

```
$ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out  
private-key.pem
```

Le paramètre `-aes256` spécifie l'algorithme utilisé pour chiffrer la clé privée. La commande renvoie la sortie suivante, y compris les invites pour définir une phrase secrète :

```
.....+++  
.+++  
Enter PEM pass phrase: xxxxxxxx  
Verifying - Enter PEM pass phrase: xxxxxxxx
```

Vous pouvez inspecter la clé publique à l'aide de la commande suivante :

```
$ openssl pkey -in private-key.pem -text
```

Cela renvoie une invite de phrase secrète et le contenu de la clé, qui devrait être similaire à ce qui suit :

```

Enter pass phrase for private-key.pem: xxxxxxxx
-----BEGIN PRIVATE KEY-----
MIIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgwgSkAgEAAoIBAQDFBXHRI4HVKAhH
3seiciooizCRTbJe1+YsXNTja4XyKypVGIFWDGhZs44FCH1P00SVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zH0SEpNmY2fMxISBxewlXr
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKK+a91K4+t03UdDR7Sno5WEXefsBrW3
g1ydo3TBsx8i5/YiV0cNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRs01AhJ
DnZPNeweboo+K3Q31wbgbm0KD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrsSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDvJXmxf0x2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGuffwXPl1i5XnpzvkdU4Hyc04zgbhXfSE
RNYjYf0GzTPwdBLpNMB6k3Tp4RHse6dNr1LH0jDhpioL8cQEBdBjyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULM1WiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjG059W
jfZjzTX5pQtVvH68rucih88DTZCwjCkjbHxg+0IkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjw1C/3jxp8zJy6P8o
JQKv7TdvMwUj4VSW0HZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1Nr0NnSz5QsndQ04Z6ihAQ1PmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEv0NK+xwUKzi9c
L/0zBq5y0IC1Pz2T85g0e1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGe0BohmF0phTHkrWKBxXiyT0oS8zjnJ1En8ysIpGg028jJr
LpaHNZ/MXQKBgQDfLncnS0LzpsS2aK0tzyZU8SMYqVH0GMxj7quhneBq2T6FbiLD
T9TV1YaGNZ0j71vQaLI19q0ubWymbautH00p5KV8owdf4+bf1/NJaPI0zhDUSiJD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycAW91Itu8aBrMndnQKBgQDb
nNp/JyRwqj0rN1jk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yu1QcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXBWdIhYyI3QKBgD+F/6wcZ85QW8nAUyKA
3WrSIx/3cwDgdm4NRGct8Z0ZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUT7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
  00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
  2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
  85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
  79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
  33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
  40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
  4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
  5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
  d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
  dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
  17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
  f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:

```

```
a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
b9
prime1:
00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
```

```

84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
38:eb:2e:96:87:35:9f:cc:5d
exponent1:
00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
06:57:6d:67:48:85:8c:88:dd
coefficient:
3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
9a:77:5a:e5:87:d5:4f:01

```

Conservez votre clé privée dans un endroit sécurisé lorsqu'elle n'est pas utilisée.

2. Générez un certificat X.509 à l'aide de la paire de clés créée à l'étape précédente. Dans cet exemple, le certificat expire dans 365 jours, après quoi il n'est plus fiable. Veillez donc à définir l'expiration de façon appropriée. Le certificat ne doit être valide que pendant la durée du processus de provisionnement. Vous pouvez supprimer le certificat du dossier de votre RIR une fois le provisionnement terminé. La commande `tr -d "\n"` supprime les caractères de nouvelle ligne (sauts de ligne) de la sortie. Vous devez fournir un nom commun lorsque vous y êtes invité, mais les autres champs peuvent être laissés vides.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
certificate.pem
```

Cela génère une sortie semblable à ce qui suit :

```
Enter pass phrase for private-key.pem: xxxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

Note

Le nom commun n'est pas nécessaire pour le AWS provisionnement. Il peut s'agir de n'importe quel nom de domaine interne ou public.

Vous pouvez inspecter le certificat à l'aide de la commande suivante :

```
$ cat certificate.pem
```

La sortie doit être une longue chaîne codée PEM sans sauts de ligne, préfacée par -----BEGIN CERTIFICATE----- et suivi de -----END CERTIFICATE-----.

2. Chargement du certificat X.509 dans l'enregistrement RDAP de votre RIR

Ajoutez le certificat que vous avez créé précédemment au registre RDAP pour votre RIR. Veillez à inclure le -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- avant et après

la partie encodée. Tout ce contenu doit se trouver sur une seule et longue ligne. La procédure de mise à jour de RDAP dépend de votre RIR :

- Pour ARIN, utilisez le [portail Account Manager](#) pour ajouter le certificat dans la section « Commentaires publics » pour l'objet « Informations réseau » représentant votre plage d'adresses. Ne l'ajoutez pas à la section des commentaires de votre organisation.
- Pour RIPE, ajoutez le certificat en tant que nouveau champ « descr » à l'objet « inetnum » ou « inet6num » représentant votre plage d'adresses. Vous les trouverez généralement dans la section « Mes ressources » du [portail de la base de données RIPE](#). Ne l'ajoutez pas dans la section des commentaires de votre organisation ni dans le champ « remarques » des objets ci-dessus.
- Pour l'APNIC, envoyez le certificat par e-mail à l'adresse helpdesk@apnic.net afin de l'ajouter manuellement au champ « remarks » (remarques) pour votre plage d'adresses. Envoyez l'e-mail en utilisant le contact autorisé APNIC pour les adresses IP.

Vous pouvez supprimer le certificat de l'enregistrement de votre RIR une fois l'étape d'allocation ci-dessous terminée.

3. Création d'un objet ROA dans votre RIR

Créez un objet ROA pour autoriser les ASN 16509 et 14618 d'Amazon à publier votre plage d'adresses et les ASN qui sont actuellement autorisés à publier la plage d'adresses. Pour le AWS GovCloud (US) Regions, autorisez l'ASN 8987 au lieu de 16509 et 14618. Vous devez définir la longueur maximale sur la taille du CIDR que vous apportez. Le préfixe IPv4 le plus spécifique que vous pouvez apporter est /24. La plage d'adresses IPv6 la plus spécifique que vous pouvez apporter est /48 pour les CIDR publiquement publiés et /56 pour les CIDR qui ne sont pas publiquement publiés.

Important

Si vous créez un objet ROA pour Amazon VPC IP Address Manager (IPAM), lorsque vous créez les ROA, pour les CIDR IPv4, vous devez définir la longueur maximale d'un préfixe d'adresse IP sur /24. Pour les CIDR IPv6, si vous les ajoutez à un groupe annoncé, la longueur maximale d'un préfixe d'adresse IP doit être /48. Cela vous garantit une flexibilité totale pour répartir votre adresse IP publique entre AWS les régions. L'IPAM applique la longueur maximale que vous avez définie. Pour plus d'informations sur les adresses BYOIP

vers IPAM, consultez [Tutoriel : BYOIP transfert des CIDR vers IPAM](#) dans le Guide de l'utilisateur Amazon VPC IPAM.

La mise à disposition de la ROA sur Amazon peut prendre jusqu'à 24 heures. Pour plus d'informations, consultez votre RIR :

- ARIN — [ROA Requests](#)
- RIPE — [Managing ROAs](#)
- APNIC — [Route Management](#)

Lorsque vous migrez des publicités d'une charge de travail sur site vers AWS, vous devez créer un ROA pour votre ASN existant avant de créer les ROA pour les ASN d'Amazon. Sinon, vous risquez de voir un impact sur votre routage et vos annonces existantes.

Important

Pour qu'Amazon puisse annoncer votre plage d'adresses IP et continuer à le faire, vos ROA avec les ASN d'Amazon doivent être conformes aux lignes directrices susmentionnées. Si vos ROA ne sont pas valides ou ne sont pas conformes aux directives ci-dessus, Amazon se réserve le droit de cesser de faire de la publicité pour votre plage d'adresses IP.

Note

Cette étape n'est pas nécessaire pour les espaces d'adressage IPv6 qui ne sont pas publiquement publiés.

Intégrer votre BYOIP

Le processus d'intégration au BYOIP comporte les tâches suivantes en fonction de vos besoins.

Tâches

- [Allocation d'une plage d'adresses publiquement publiée dans AWS](#)
- [Allocation d'une plage d'adresses IPv6 qui n'est pas publiquement publiée](#)
- [Faites connaître la plage d'adresses via AWS](#)

- [Mise hors service de la plage d'adresses](#)

Allocation d'une plage d'adresses publiquement publiée dans AWS

Lorsque vous configurez une plage d'adresses à utiliser avec AWS, vous confirmez que vous contrôlez la plage d'adresses et que vous autorisez Amazon à en faire la publicité. Nous vérifions également que vous contrôlez la plage d'adresses via un message d'autorisation signé. Ce message est signé avec la paire de clés X.509 auto-signée que vous avez utilisée lors de la mise à jour de l'enregistrement RDAP avec le certificat X.509. AWS nécessite un message d'autorisation signé cryptographiquement qu'il présente au RIR. Le RIR authentifie la signature par rapport au certificat que vous avez ajouté au RDAP et vérifie les détails d'autorisation par rapport au ROA.

Pour allouer la plage d'adresses

1. Composer un message

Composez le message d'autorisation en texte brut. Le format du message est le suivant, où la date est la date d'expiration du message :

```
1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
```

Remplacez le numéro de compte, la plage d'adresses et la date d'expiration par vos propres valeurs pour créer un message semblable au suivant :

```
text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
```

Cela ne doit pas être confondu avec un message ROA, qui a une apparence similaire.

2. Signer un message

Signez le message en texte brut à l'aide de la clé privée que vous avez créée précédemment. La signature renvoyée par cette commande est une longue chaîne que vous devrez utiliser à l'étape suivante.

Important

Nous vous recommandons de copier et de coller cette commande. À l'exception du contenu du message, ne modifiez ni ne remplacez aucune des valeurs.

```
signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt  
rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM  
| openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
```

3. Approvisionner une adresse

Utilisez la commande AWS CLI [provision-byoip-cidr](#) pour provisionner la plage d'adresses. La commande `--cidr-authorization-context` utilise les chaînes de message et de signature que vous avez créées précédemment.

Important

Vous devez spécifier la AWS région dans laquelle la plage BYOIP doit être provisionnée si elle diffère de votre configuration. `AWS CLI Default region name`

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context  
Message="$text_message",Signature="$signed_message" --region us-east-1
```

La mise en service d'une plage d'adresses est une opération asynchrone : l'appel est immédiatement renvoyé, mais la plage d'adresses ne peut pas être utilisée tant que son statut ne bascule pas de `pending-provision` à `provisioned`.

4. Surveiller la progression

Bien que la plupart des approvisionnements soient effectués dans les deux heures, le processus d'approvisionnement pour les gammes pouvant faire l'objet d'une publicité publique peut prendre jusqu'à une semaine. Utilisez la commande [describe-byoip-cidrs](#) pour surveiller la progression, comme dans cet exemple :

```
aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
```

S'il y a des problèmes pendant la mise en service et que l'état passe à `failed-provision`, vous devez exécuter à nouveau la commande `provision-byoip-cidr` une fois que les problèmes ont été résolus.

Allocation d'une plage d'adresses IPv6 qui n'est pas publiquement publiée

Par défaut, une plage d'adresses est allouée pour être publiquement publiée sur Internet. Vous pouvez allouer une plage d'adresses IPv6 qui ne sera pas publiquement publiée. Pour les acheminements qui ne sont pas publiquement annoncés, le processus d'approvisionnement se termine généralement en quelques minutes. Lorsque vous associez un bloc d'adresses CIDR IPv6 d'une plage d'adresses non publique à un VPC, le CIDR IPv6 ne peut être accessible que via les options de connectivité hybride prenant en charge IPv6, telles que [AWS Direct Connect](#), [AWS Site-to-Site VPN](#), ou les [passerelles Transit Gateway d'Amazon VPC](#).

Un ROA n'est pas nécessaire pour fournir une plage d'adresses non publique.

Important

- Vous ne pouvez spécifier si une plage d'adresses est publiquement publiée que pendant l'allocation. Vous ne pouvez pas modifier l'état annoncé ultérieurement.
- Amazon VPC ne prend pas en charge les CIDR à [adresse locale unique](#) (ULA). Tous les VPC doivent disposer de CIDR IPv6 uniques. Deux VPC ne peuvent pas avoir la même plage d'adresses CIDR IPv6.

Pour provisionner une plage d'adresses IPv6 qui ne sera pas publiquement publiée, utilisez la commande [provision-byoip-cidr](#) suivante.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context  
Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --  
region us-east-1
```

Faites connaître la plage d'adresses via AWS

Une fois que la plage d'adresses est mise en service, elle est prête à être publiée. Vous devez publier la plage d'adresses exacte que vous avez mise en service. Vous ne pouvez pas publier seulement une portion de la plage d'adresses mise en service.

Si vous avez provisionné une plage d'adresses IPv6 qui ne sera pas publiée publiquement, vous n'avez pas besoin de terminer cette étape.

Nous vous recommandons de cesser de faire de la publicité pour la plage d'adresses ou toute partie de cette plage depuis d'autres sites avant de la diffuser AWS. Si vous continuez à faire de la publicité

pour votre plage d'adresses IP, en tout ou en partie, à partir d'autres sites, nous ne serons pas en mesure de fournir une assistance fiable ou de résoudre les problèmes. Plus précisément, nous ne pouvons pas garantir que le trafic vers la plage d'adresses ou une partie de cette plage entrera dans notre réseau.

Pour minimiser les temps d'arrêt, vous pouvez configurer vos AWS ressources pour utiliser une adresse de votre pool d'adresses avant qu'elle ne soit publiée, puis arrêter de la publier depuis son emplacement actuel et commencer à en faire la publicité par le biais AWS de cette adresse. Pour plus d'informations sur l'allocation d'une adresse IP Elastic à partir de votre groupe d'adresses, consultez [allouer une adresse IP Elastic](#) ;.

Limites

- Vous pouvez exécuter la commande `advertise-byoip-cidr` au moins une fois tous les 10 secondes, même si vous spécifiez des plages d'adresses différentes à chaque fois.
- Vous pouvez exécuter la commande `withdraw-byoip-cidr` au moins une fois tous les 10 secondes, même si vous spécifiez des plages d'adresses différentes à chaque fois.

Pour publier la plage d'adresses, utilisez la commande [advertise-byoip-cidr](#) suivante.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Pour arrêter la publication de la plage d'adresses, utilisez la commande [withdraw-byoip-cidr](#) suivante.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Mise hors service de la plage d'adresses

Pour arrêter d'utiliser votre plage d'adresses AWS, libérez d'abord toutes les adresses IP élastiques et dissociez tous les blocs d'adresse CIDR IPv6 encore alloués du pool d'adresses. Ensuite, arrêtez la publicité de la plage d'adresses et enfin, mettez hors service la plage d'adresses.

Vous ne pouvez pas mettre hors service une partie de la plage d'adresses. Si vous souhaitez utiliser une plage d'adresses plus spécifique avec AWS, déprovisionnez l'ensemble de la plage d'adresses et configurez une plage d'adresses plus spécifique.

Pour libérer chaque adresse IP Elastic, utilisez la commande [release-address](#) suivante.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Pour dissocier un bloc CIDR IPv6, utilisez la commande [disassociate-vpc-cidr-block](#) suivante.

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
--region us-east-1
```

Pour arrêter la publication de la plage d'adresses, utilisez la commande [withdraw-byoip-cidr](#) suivante.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Pour annuler l'allocation de la plage d'adresses, utilisez la commande [deprovision-byoip-cidr](#) suivante.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

La mise hors service d'une plage d'adresses peut prendre jusqu'à un jour.

Utiliser votre plage d'adresses

Vous pouvez afficher et utiliser les plages d'adresses IPv4 et IPv6 que vous avez approvisionnées dans votre compte.

Plages d'adresses IPv4

Vous pouvez créer une adresse IP élastique à partir de votre pool d'adresses IPv4 et l'utiliser avec vos AWS ressources, telles que les instances EC2, les passerelles NAT et les équilibreurs de charge réseau.

Pour afficher des informations sur les pools d'adresses IPv4 que vous avez provisionnés dans votre compte, utilisez la commande [describe-public-ipv4-pools](#) suivante.

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Pour créer une adresse IP Elastic à partir de votre pool d'adresses, utilisez la commande [allocate-address](#). Vous pouvez utiliser l'option `--public-ipv4-pool` pour spécifier l'ID du groupe d'adresses renvoyé par `describe-byoip-cidrs`. Vous pouvez aussi utiliser l'option `--address` pour spécifier une adresse de la plage d'adresses que vous avez allouée.

Plages d'adresses IPv6

Pour afficher des informations sur les pools d'adresses IPv6 que vous avez provisionnés dans votre compte, utilisez la commande [describe-ipv6-pools](#) suivante.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Pour créer un VPC et spécifier un CIDR IPv6 à partir de votre pool d'adresses IPv6, utilisez la commande [create-vpc](#) suivante. Pour laisser Amazon choisir le CIDR IPv6 dans votre pool d'adresses IPv6, omettez l'option `--ipv6-cidr-block`.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-pool pool-id --region us-east-1
```

Pour associer un bloc CIDR IPv6 de votre pool d'adresses IPv6 à un VPC, utilisez la commande [associate-vpc-cidr-block](#) suivante. Pour laisser Amazon choisir le CIDR IPv6 dans votre pool d'adresses IPv6, omettez l'option `--ipv6-cidr-block`.

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-cidr --ipv6-pool pool-id --region us-east-1
```

Pour afficher vos VPC et les informations de pool d'adresses IPv6 associées, utilisez la commande [describe-vpcs](#) . Pour afficher des informations sur les blocs CIDR IPv6 associés à partir d'un pool d'adresses IPv6 spécifique, utilisez la commande [get-associated-ipv6-pool-cidrs](#) suivante.

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Si vous dissociez le bloc CIDR IPv6 de votre VPC, il est libéré dans votre pool d'adresses IPv6.

Valider votre BYOIP

1. Valider la paire de clés x.509 auto-signée

Vérifiez que le certificat a été chargé et est valide via la commande `whois`.

Pour ARIN, utilisez `whois -h whois.arin.net r + 2001:0DB8:6172::/48` pour rechercher le registre RDAP pour votre plage d'adresses. Recherchez la NetRange (plage réseau) dans la section `Public Comments` dans la sortie de commande. Le certificat doit être ajouté dans la section `Public Comments` pour la plage d'adresses.

Vous pouvez inspecter le `Public Comments` contenant le certificat à l'aide de la commande suivante :

```
whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
```

Cela renvoie une sortie avec le contenu de la clé, qui devrait être similaire à ce qui suit :

```
Public Comments:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAGMCEf1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFd1YiBTZXJ2aWN1czETMBEGA1UEC
wwKQ11PSVAgRGVtbzETMBEGA1UEAwwKQ11PSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpviBXZWIgU2
Vydm1jZXMxEzARBGNVBAsMCKJZT0lQIERlbW8xEzARBGNVBAMMCKJZT0lQIERlb
W8wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqur9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QeshVRw0aXUdprAnndaTug
mDPkD0vr1475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wX1AqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdEiW48QaYjhM1UEf
xdaqYUinz8KpjfADZ4Hvqj9jWZ/eXo/9b2rG1HWkJsbhr0VEUYAGu1bwkgcdww
3A7Nj0xQbAgMBAAGjUzBRMB0GA1UdDgQWBBSStFyujN6SYBr2g1HpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2g1HpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQB6nn6YLh5211fyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0c1r00aFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVz0yt6fPzj0vJLcsqc1hcF9wySL507XQz76Uk5cFypB0zbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvphdSGCvRD1/qd0/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIs0NPYqrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Pour RIPE, utilisez `whois -r -h whois.ripe.net 2001:0DB8:7269::/48` pour rechercher le registre RDAP pour votre plage d'adresses. Recherchez l'objet `inetnum` (plage réseau) dans la section `descr` dans la sortie de commande. Le certificat doit être ajouté en tant que nouveau champ `descr` pour la plage d'adresses.

Vous pouvez inspecter le `descr` contenant le certificat à l'aide de la commande suivante :

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Cela renvoie une sortie avec le contenu de la clé, qui devrait être similaire à ce qui suit :

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCT1oxETAPBgNVBAG
MCEf1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
d1YiBTZXJ2aWN1czETMBEGA1UECwwKQ11PSVAgRGVtbzETMBEGA1UEAwwKQ11PS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBGNVBAoME0FtYXpviBXZWIgU2Vydm1jZXNxEzARBGNVBAsMCKJZT01QIERlbW
8xEzARBGNVBAMMCKJZT01QIERlbW8wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqfR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jSWhWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QeshVRw0aXUdprAnndaTugmDPKD0vr1475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wX1AqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdEiW48QaYjhM1UEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
G1HwkJsbhr0VEUyAGu1bWkgcdww3A7Nj0xQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2g1HpGt0XGF7GbgTAFBGNVHSMEGDAWgBSTFyujN6SYBr2g1HpGt0
XGF7GbgTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwJAA4IBAQBx6nn6Y
Lhz5211fyVfxY0t6o3410bQAEAF08ud+ICtmQ4IO4A4B7zV3zIVYr0c1r00aFyL
xngwMYN0XY5tVhdQqk4/gmDNEKSzy2QkX4Eg0YUWVz0yt6fPzj0vJLcsqc1hcF9
wySL507XQz76Uk5cFypB0zbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRD1/qd0/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj81Thoar17Uo9y/Q5qJIs0N
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Pour APNIC, utilisez `whois -h whois.apnic.net 2001:0DB8:6170::/48` pour rechercher le registre RDAP pour votre plage d'adresses BYOIP. Recherchez l'objet `inetnum` (plage réseau) dans la section `remarks` dans la sortie de commande. Le certificat doit être ajouté en tant que nouveau champ `remarks` pour la plage d'adresses.

Vous pouvez inspecter le `remarks` contenant le certificat à l'aide de la commande suivante :

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Cela renvoie une sortie avec le contenu de la clé, qui devrait être similaire à ce qui suit :

```
remarks:
-----BEGIN CERTIFICATE-----
```

```

MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAGMCEf1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWN1czETMBEGA1UEC
wwKQ11PSVAgRGVtbzETMBEGA1UEAwwKQ11PSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvcjBiXZWIgU2
Vydm1jZXMxEzARBGNVBA5MCKJZT01QIER1bW8xEzARBGNVBAMMKJZT01QIER1b
W8wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqurfR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRw0aXUdprAnndaTug
mDPkD0vr1475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wX1AqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdEiW48QaYjhM1UEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rG1HWkJsbhR0VEUyAGu1bwkgcdww
3A7Nj0xQbAgMBAAGjUzBRMB0GA1UdDgQWBBSstFyujN6SYBr2g1HpGt0XGF7GbGT
AfBgNVHSMEGDAWgBSstFyujN6SYBr2g1HpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBx6nn6YLhZ5211fyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0c1r00aFyLxngwMYN0XY5tVhdQqk4/gmDNEKS
Zy2QkX4Eg0YUWVz0yt6fPzj0vJLcsqc1hcF9wySL507XQz76Uk5cFypB0zbnk35
UkWrzaA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarimmy2vtWBxwrqkFvphSGCvRD1/qd0/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIs0NPYqrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----

```

2. Valider la création d'un objet ROA

Validez la création réussie des objets ROA à l'aide de l'API de données RIPEstat. Assurez-vous de tester votre plage d'adresses par rapport aux ASN 16509 et 14618 d'Amazon, ainsi que les ASN qui sont actuellement autorisés à publier la plage d'adresses.

Vous pouvez inspecter les objets ROA provenant de différents ASN d'Amazon avec votre plage d'adresses à l'aide de la commande suivante :

```

curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
resource=ASN&prefix=CIDR

```

Dans cet exemple de sortie, la réponse a un résultat de "status": "valid" pour l'ASN 16509 d'Amazon. Cela indique que l'objet ROA de la plage d'adresses a été créé avec succès :

```

{
  "messages": [],
  "see_also": [],
  "version": "0.3",

```

```
"data_call_name": "rpki-validation",
"data_call_status": "supported",
"cached": false,
"data": {
  "validating_roas": [
    {
      "origin": "16509",
      "prefix": "2001:0DB8::/32",
      "max_length": 48,
      "validity": "valid"
    },
    {
      "origin": "14618",
      "prefix": "2001:0DB8::/32",
      "max_length": 48,
      "validity": "invalid_asn"
    },
    {
      "origin": "64496",
      "prefix": "2001:0DB8::/32",
      "max_length": 48,
      "validity": "invalid_asn"
    }
  ],
  "status": "valid",
  "validator": "routinator",
  "resource": "16509",
  "prefix": "2001:0DB8::/32"
},
"query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
"process_time": 58,
"server_id": "app116",
"build_version": "live.2023.2.1.142",
"status": "ok",
"status_code": 200,
"time": "2023-02-24T15:24:30.773654"
}
```

Le statut “unknown” indique que l’objet ROA de la plage d’adresses n’a pas été créé. Le statut “invalid_asn” indique que l’objet ROA de la plage d’adresses n’a pas été créé avec succès.

Disponibilité par région

La fonctionnalité BYOIP est actuellement disponible dans toutes les [régions AWS commerciales](#) à l'exception des régions chinoises.

Disponibilité de la zone locale

Une [zone locale](#) est une extension d'une AWS région située à proximité géographique de vos utilisateurs. Les Zones Locales sont regroupées en « groupes de frontières réseau ». Dans AWS, un groupe frontalier du réseau est un ensemble de zones de disponibilité (AZ), de zones locales ou de zones de longueur d'onde à partir desquelles AWS une adresse IP publique est annoncée. Les zones locales peuvent avoir des groupes de frontières de réseau différents de ceux des zones de disponibilité d'une AWS région afin de garantir une latence minimale ou une distance physique minimale entre le AWS réseau et les clients accédant aux ressources de ces zones.

Vous pouvez fournir des plages d'adresses BYOIPv4 et les publier dans les groupes frontaliers du réseau de zone locale suivants à l'aide de l'option `--network-border-group` :

- us-east-1-dfw-2
- us-west-2-lax-1
- us-west-2-phx-2

Si vous avez des zones locales activées (voir [Enable a Local Zone](#)), vous pouvez choisir un groupe de frontières réseau pour les zones locales lorsque vous allouez et publiez un CIDR BYOIPv4. Choisissez soigneusement le groupe de bordure du réseau car l'EIP et la AWS ressource à laquelle il est associé doivent résider dans le même groupe de bordure du réseau.

Note

Vous ne pouvez pas allouer ou publier des plages d'adresses BYOIPv6 dans les zones locales pour le moment.

En savoir plus

Pour plus d'informations, consultez le débat technique AWS en ligne [sur le thème « Bring Your Own IP »](#).

Adresses IP Elastic

Une adresse IP Elastic est une adresse IP IPv4 statique conçue pour le cloud computing. Une adresse IP élastique est attribuée à votre AWS compte et vous appartient jusqu'à ce que vous la publiiez. En utilisant une adresse IP Elastic, vous pouvez contourner un problème de défaillance d'une instance ou d'un logiciel en remappant rapidement l'adresse à une autre instance de votre compte. Vous pouvez également spécifier l'adresse IP Elastic dans un enregistrement DNS pour votre domaine, de sorte que votre domaine pointe vers votre instance. Pour plus d'informations, consultez la documentation de votre bureau d'enregistrement de domaines.

Une adresse IP Elastic est une adresse IP IPv4 publique, qui est accessible depuis Internet. Si votre instance ne dispose pas d'une adresse IPv4 publique, vous pouvez lui associer une adresse IP Elastic pour établir la communication avec Internet. Cela vous permet, par exemple, de vous connecter à l'instance à partir de votre ordinateur local.

Table des matières

- [Tarification des adresses IP Elastic](#)
- [Principes de base d'une adresse IP Elastic](#)
- [Utiliser des adresses IP Elastic](#)
- [Quota appliqué aux adresses IP Elastic](#)

Tarification des adresses IP Elastic

AWS frais pour toutes les adresses IPv4 publiques, y compris les adresses IPv4 publiques associées aux instances en cours d'exécution et les adresses IP Elastic. Pour plus d'informations, consultez l'onglet Adresse IPv4 publique de la [page de tarification d'Amazon VPC](#).

Principes de base d'une adresse IP Elastic

Les caractéristiques de base d'une adresse IP Elastic sont les suivantes :

- Une adresse IP Elastic est statique ; elle ne change pas au fil du temps.
- Une adresse IP Elastic est destinée uniquement à une région spécifique et ne peut pas être déplacée vers une autre région.
- Une adresse IP élastique provient du pool d'adresses IPv4 d'Amazon ou d'un pool d'adresses IPv4 personnalisé que vous avez intégré à votre AWS compte.

- Pour utiliser une adresse IP Elastic, commencez par en attribuer une à votre compte, puis associez-la à votre instance ou à une interface réseau.
- Lorsque vous associez une adresse IP Elastic à une instance, elle est également associée à l'interface réseau principale de l'instance. Lorsque vous associez une adresse IP Elastic à une interface réseau attachée à une instance, elle est également associée à l'instance.
- Lorsque vous associez une adresse IP élastique à une instance ou à son interface réseau principale, si l'instance est déjà associée à une adresse IPv4 publique, cette adresse IPv4 publique est réintégrée dans le pool d'adresses IPv4 publiques d'Amazon et l'adresse IP élastique est associée à l'instance à la place. Vous ne pouvez pas réutiliser l'adresse IPv4 publique précédemment associée à l'instance et vous ne pouvez pas convertir cette adresse IPv4 publique en adresse IP élastique. Pour plus d'informations, consultez [Adresses IPv4 publiques](#).
- Vous pouvez dissocier une adresse IP Elastic d'une ressource et la réassocier à une autre ressource. Pour éviter un comportement inattendu, assurez-vous que toutes les connexions actives à la ressource nommée dans l'association existante sont fermées avant d'effectuer la modification. Une fois que vous avez associé votre adresse IP Elastic à une ressource différente, vous pouvez rouvrir vos connexions à la ressource nouvellement associée.
- Une adresse IP Elastic dissociée demeure attribuée à votre compte jusqu'à ce que vous la libériez explicitement. Toutes les adresses IP Elastic de votre compte vous sont facturées, qu'elles soient associées ou non à une instance. Pour plus d'informations, consultez l'onglet Adresse IPv4 publique de la [page de tarification d'Amazon VPC](#).
- Lorsque vous associez une adresse IP Elastic à une instance qui avait une adresse IPv4 publique, le nom d'hôte DNS public de l'instance est mis à jour pour correspondre à l'adresse IP Elastic.
- Nous résolvons un nom d'hôte DNS public en adresse IPv4 publique ou en l'adresse IP Elastic de l'instance en dehors du réseau de cette dernière et nous la résolvons en adresse IPv4 privée de l'instance depuis le réseau de cette dernière.
- Lorsque vous attribuez une adresse IP élastique à partir d'un pool d'adresses IP que vous avez ajouté à votre AWS compte, elle n'est pas prise en compte dans le calcul de vos limites d'adresses IP élastiques. Pour plus d'informations, consultez [Quota appliqué aux adresses IP Elastic](#).
- Lorsque vous allouez les adresses IP Elastic, vous pouvez les associer à un groupe de bordure réseau. C'est l'endroit à partir duquel nous publions le bloc d'adresses CIDR. La définition du groupe de bordure réseau limite le bloc d'adresses CIDR à ce groupe. Si vous ne spécifiez pas le groupe de bordure réseau, nous définissons le groupe de bordure contenant toutes les zones de disponibilité de la région (par exemple, us-west-2).
- Une adresse IP Elastic ne peut être utilisée que dans un groupe de frontière de réseau spécifique.

Utiliser des adresses IP Elastic

Les sections suivantes expliquent comment utiliser les adresses IP Elastic.

Tâches

- [allouer une adresse IP Elastic](#) ;
- [Décrire vos adresses IP Elastic](#)
- [Baliser une adresse IP Elastic](#)
- [Associer une adresse IP Elastic à une instance ou une interface réseau](#)
- [Dissocier une adresse IP Elastic](#)
- [Transfert d'adresses IP Elastic](#)
- [Libérer une adresse IP Elastic](#)
- [Récupérer une adresse IP Elastic](#)
- [Utiliser des enregistrements DNS inverses pour les applications de messagerie](#)

allouer une adresse IP Elastic ;

Vous pouvez attribuer une adresse IP élastique à partir du pool d'adresses IPv4 publiques d'Amazon ou d'un pool d'adresses IP personnalisé que vous avez intégré à votre AWS compte. Pour plus d'informations sur l'ajout de votre propre plage d'adresses IP à votre AWS compte, consultez [Fourniture de vos propres adresses IP \(BYOIP\) dans Amazon EC2](#).

Vous pouvez allouer une adresse IP Elastic à l'aide de l'une des méthodes suivantes.

Console

Pour allouer une adresse IP Elastic

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Réseau et sécurité, Adresses IP Elastic.
3. Choisissez Allocate Elastic IP address (Allouer l'adresse IP Elastic).
4. (Facultatif) Lorsque vous allouez une adresse IP Elastic (EIP), vous choisissez le Groupe de bordures réseau dans lequel vous souhaitez allouer l'EIP. Un groupe frontalier réseau est un ensemble de zones de disponibilité (AZ), de zones Locales ou de zones de longueur d'onde à partir AWS duquel est annoncée une adresse IP publique. Les zones Locales et les Zones de longueur d'onde peuvent avoir des groupes de frontières de réseau différents de ceux

des zones de disponibilité d'une région afin de garantir une latence minimale ou une distance physique minimale entre le AWS réseau et les clients accédant aux ressources de ces zones.

⚠ Important

Vous devez allouer un EIP dans le même groupe frontalier du réseau que la AWS ressource qui sera associée à l'EIP. Une EIP appartenant à un groupe de bordures réseau ne peut être annoncée que dans les zones de ce groupe de bordures réseau et dans aucune autre zone représentée par d'autres groupes de bordures réseau.

Si vous avez des zones locales ou des zones Wavelength qui sont activées (pour plus d'informations, consultez [Enable a Local Zone](#) ou [Enable Wavelength Zones](#)), vous pouvez choisir un groupe de bordures réseau pour les zones de disponibilité, les zones locales ou les zones Wavelength. Choisissez le groupe de bordures réseau avec soin, car l'EIP et la ressource AWS à laquelle elle est associée doivent résider dans le même groupe de bordures réseau. Vous pouvez utiliser la console EC2 pour afficher le groupe frontalier du réseau dans lequel se trouvent vos zones de disponibilité, zones locales ou zones de longueur d'onde. En général, toutes les zones de disponibilité d'une région appartiennent au même groupe de bordures réseau, tandis que les zones locales ou les zones Wavelength appartiennent à leurs propres groupes de bordures réseau distincts.

Si vous n'avez pas de zones locales ou de zones Wavelength activées, lorsque vous allouez une EIP, le groupe de bordures réseau qui représente toutes les zones de disponibilité de la région (par exemple, us-west-2) est prédéfini pour vous et vous ne pouvez pas le modifier. Cela signifie que l'EIP que vous allouez à ce groupe de bordures réseau sera annoncée dans toutes les zones de disponibilité de la région dans laquelle vous vous trouvez.

5. Pour Pool d'adresses IPv4 publiques, choisissez l'une des options suivantes :
 - Amazon's pool of IPv4 addresses (Groupe d'adresses IPv4 d'Amazon)—À utiliser si vous souhaitez qu'une adresse IPv4 soit allouée à partir du groupe d'adresses IP d'Amazon.
 - Adresse IPv4 publique que vous apportez à votre AWS compte : si vous souhaitez attribuer une adresse IPv4 à partir d'un pool d'adresses IP que vous avez intégré à votre compte. AWS Cette option est désactivée si vous ne disposez pas de groupes d'adresses IP.
 - Groupe d'adresses IPv4 appartenant au client : si vous souhaitez allouer une adresse IPv4 depuis un groupe créé à partir de votre réseau sur site pour une utilisation avec un Outpost AWS . Cette option est désactivée si vous n'avez pas d' AWS avant-poste.

6. (Facultatif) Ajoutez ou supprimez une balise.

[Ajouter une balise] Choisissez Ajouter une nouvelle balise et procédez comme suit :

- Pour Clé, saisissez le nom de la clé.
- Pour Value (Valeur), saisissez la valeur de clé.

[Supprimer une balise] Choisissez Supprimer à la droite de la clé et de la valeur de la balise.

7. Choisissez Allocate.

AWS CLI

Pour allouer une adresse IP Elastic

Utilisez la commande [allocate-address](#) de l' AWS CLI .

PowerShell

Pour allouer une adresse IP Elastic

Utilisez la [New-EC2Address](#) AWS Tools for Windows PowerShell commande.

Décrire vos adresses IP Elastic

Vous pouvez décrire une adresse IP Elastic à l'aide de l'une des méthodes suivantes.

Console

Pour décrire vos adresses IP Elastic

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic à afficher, puis choisissez Actions, View details (Afficher les détails).

AWS CLI

Pour décrire vos adresses IP Elastic

Utilisez la commande [describe-addresses](#) AWS CLI .

PowerShell

Pour décrire vos adresses IP Elastic

Utilisez la [Get-EC2Address](#) AWS Tools for Windows PowerShell commande.

Baliser une adresse IP Elastic

Vous pouvez allouer des balises personnalisées à vos adresses IP Elastic pour classer celles-ci de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Cela vous aide à retrouver rapidement une adresse IP Elastic spécifique en fonction des balises personnalisées que vous lui avez attribuées.

Le suivi d'allocation des coûts à l'aide des balises d'adresse IP Elastic n'est pas pris en charge.

Vous pouvez baliser une adresse IP Elastic à l'aide de l'une des méthodes suivantes.

Console

Pour baliser une adresse IP Elastic

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic à baliser, puis choisissez Actions, View details (Afficher les détails).
4. Dans la section Tags (Balises) choisissez Manage tags (Gérer les balises).
5. Spécifiez une paire de clé et de valeur de balise.
6. (Facultatif) Choisissez Add tag (Ajouter une balise) pour ajouter des balises supplémentaires.
7. Choisissez Enregistrer.

AWS CLI

Pour baliser une adresse IP Elastic

Utilisez la commande [create-tags](#) AWS CLI .

```
aws ec2 create-tags --resources eipalloc-12345678 --tags Key=Owner,Value=TeamA
```

PowerShell

Pour baliser une adresse IP Elastic

Utilisez la [New-EC2Tag](#) AWS Tools for Windows PowerShell commande.

La commande New-EC2Tag nécessite un paramètre Tag, qui spécifie la paire clé-valeur à utiliser pour la balise d'adresse IP Elastic. Les commandes suivantes créent le paramètre Tag :

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource eipalloc-12345678 -Tag $tag
```

Associer une adresse IP Elastic à une instance ou une interface réseau

Si vous associez une adresse IP Elastic à votre instance pour permettre la communication avec Internet, vous devez également vous assurer que votre instance se trouve dans un sous-réseau public. Pour plus d'informations, consultez [Passerelles Internet](#) dans le Guide de l'utilisateur Amazon VPC.

Vous pouvez associer une adresse IP Elastic à une instance ou à une interface réseau à l'aide de l'une des méthodes suivantes.

Console

Pour associer une adresse IP Elastic à une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic à associer, puis choisissez Actions, Associate Elastic IP address (Associer l'adresse IP Elastic).
4. Pour Resource type (Type de ressource), choisissez Instance.
5. Par exemple, choisissez l'instance à laquelle vous souhaitez associer l'adresse IP Elastic. Vous pouvez également entrer du texte pour rechercher une instance spécifique.
6. (Facultatif) Pour Private IP address (Adresse IP privée), spécifiez une adresse IP privée à laquelle associer l'adresse IP Elastic.

7. Choisissez Associate.

Pour associer une adresse IP Elastic à une interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic à associer, puis choisissez Actions, Associate Elastic IP address (Associer l'adresse IP Elastic).
4. Pour Type de ressource, choisissez Interface réseau.
5. Dans Network interface (Interface réseau), choisissez l'interface réseau à laquelle associer l'adresse IP Elastic. Vous pouvez également entrer du texte pour rechercher une interface réseau spécifique.
6. (Facultatif) Pour Private IP address (Adresse IP privée), spécifiez une adresse IP privée à laquelle associer l'adresse IP Elastic.
7. Choisissez Associate.

AWS CLI

Pour associer une adresse IP Elastic

Utilisez la commande [associate-address](#) AWS CLI .

PowerShell

Pour associer une adresse IP Elastic

Utilisez la [Register-EC2Address](#) AWS Tools for Windows PowerShell commande.

Dissocier une adresse IP Elastic

Vous pouvez dissocier une adresse IP Elastic d'une instance ou d'une interface réseau à tout moment. Après avoir dissocié l'adresse IP Elastic, vous pouvez la réassocier à une autre ressource.

Vous pouvez dissocier une adresse IP Elastic à l'aide de l'une des méthodes suivantes.

Console

Pour dissocier et réassocier une adresse IP Elastic

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic à dissocier, puis choisissez Actions, Disassociate Elastic IP address (Dissocier l'adresse IP Elastic).
4. Choisissez Dissocier.

AWS CLI

Dissocier une adresse IP Elastic

Utilisez la commande [disassociate-address](#) AWS CLI .

PowerShell

Dissocier une adresse IP Elastic

Utilisez la commande [Unregister-EC2Address](#). AWS Tools for Windows PowerShell

Transfert d'adresses IP Elastic

Cette section décrit comment transférer des adresses IP Elastic d'un compte Compte AWS à un autre. Le transfert d'adresses IP Elastic peut être utile dans les situations suivantes :

- Restructuration organisationnelle : utilisez les transferts d'adresses IP élastiques pour déplacer rapidement les charges de travail de l'une Compte AWS à l'autre. Vous n'avez pas besoin d'attendre que les nouvelles adresses IP Elastic soient autorisées dans vos groupes de sécurité et vos NACL.
- Administration centralisée de la sécurité : utilisez un compte AWS de sécurité centralisé pour suivre et transférer les adresses IP élastiques dont la conformité en matière de sécurité a été vérifiée.
- Reprise après sinistre : utilisez les transferts d'adresses IP Elastic pour remapper rapidement les adresses IP des charges de travail Internet accessibles au public dans les situations d'urgence.

Le transfert d'adresses IP Elastic est gratuit.

Tâches

- [Activation du transfert d'adresses IP Elastic](#)
- [Désactivation du transfert d'adresses IP Elastic](#)
- [Acceptation d'une adresse IP Elastic transférée](#)

Activation du transfert d'adresses IP Elastic

Cette section décrit comment accepter une adresse IP Elastic transférée. Notez les limitations suivantes en ce qui concerne l'activation des adresses IP Elastic pour le transfert :

- Vous pouvez transférer des adresses IP élastiques de n'importe quel Compte AWS (compte source) vers n'importe quel autre AWS compte de la même AWS région (compte de transfert).
- Lorsque vous transférez une adresse IP Elastic, il existe une liaison en deux étapes entre les Comptes AWS. Lorsque le compte source lance le transfert, les comptes de transfert ont sept jours pour accepter le transfert de l'adresse IP Elastic. Pendant ces sept jours, le compte source peut consulter le transfert en attente (par exemple dans la AWS console ou à l'aide de la commande [AWS CLI describe-address-transfers](#)). Au bout de sept jours, le transfert expire et la propriété de l'adresse IP Elastic revient au compte source.
- Les transferts acceptés sont visibles sur le compte source (par exemple dans la AWS console ou à l'aide de la AWS CLI commande [describe-address-transfers](#)) pendant trois jours après leur acceptation.
- AWS n'informe pas les comptes de transfert des demandes de transfert d'adresse IP Elastic en attente. Le propriétaire du compte source doit informer le propriétaire du compte de transfert qu'il doit accepter une demande de transfert d'adresse IP Elastic.
- Toutes les balises associées à une adresse IP Elastic en cours de transfert sont réinitialisées lorsque le transfert est terminé.
- Vous ne pouvez pas transférer les adresses IP élastiques allouées à partir de pools d'adresses IPv4 publics que vous apportez à votre Compte AWS compte, communément appelés pools d'adresses BYOIP (Bring Your Own IP).
- Si vous tentez de transférer une adresse IP Elastic à laquelle est associé un enregistrement DNS inversé, vous pouvez lancer le processus de transfert, mais le compte de transfert ne sera pas en mesure de l'accepter tant que l'enregistrement DNS associé n'aura pas été supprimé.
- Si vous avez activé et configuré AWS Outposts, vous avez peut-être alloué des adresses IP élastiques à partir d'un pool d'adresses IP (CoIP) appartenant au client. Vous ne pouvez pas transférer des adresses IP Elastic attribuées à partir d'un groupe CoIP. Cependant, vous pouvez

l'utiliser AWS RAM pour partager une CoIP avec un autre compte. Pour plus d'informations, voir [Adresses IP appartenant au client](#) dans le Guide de l'utilisateur AWS Outposts .

- Vous pouvez utiliser Amazon VPC IPAM pour suivre le transfert d'adresses IP Elastic vers les comptes d'une organisation depuis AWS Organizations. Pour plus d'informations, voir [Afficher l'historique des adresses IP](#). Cependant, si une adresse IP Elastic est transférée vers un compte Compte AWS en dehors de l'organisation, l'historique d'audit IPAM de l'adresse IP Elastic sera perdu.

Cette procédure doit être suivie par le compte source.

Console

Pour activer le transfert d'adresses IP Elastic

1. Assurez-vous d'utiliser le AWS compte source.
2. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
3. Dans le panneau de navigation, choisissez Adresses IP Elastic.
4. Sélectionnez une ou plusieurs adresses IP Elastic à activer pour le transfert, puis choisissez Actions, Enable transfer (Activer le transfert).
5. Si vous transférez plusieurs adresses IP Elastic, l'option Transfer type (Type de transfert) s'affiche. Choisissez l'une des options suivantes :
 - Choisissez Compte unique si vous transférez les adresses IP élastiques vers un seul AWS compte.
 - Choisissez Plusieurs comptes si vous transférez les adresses IP élastiques vers plusieurs AWS comptes.
6. Dans Transfer account ID (ID de compte de transfert), saisissez les ID des comptes AWS vers lesquels vous souhaitez transférer les adresses IP Elastic.
7. Confirmez le transfert en saisissant **enable** dans la zone de texte.
8. Sélectionnez Envoyer.
9. Pour accepter le transfert, voir [Acceptation d'une adresse IP Elastic transférée](#). Pour désactiver le transfert, voir [Désactivation du transfert d'adresses IP Elastic](#).

AWS CLI

Pour activer le transfert d'adresses IP Elastic

Utilisez la commande [enable-address-transfer](#).

PowerShell

Pour activer le transfert d'adresses IP Elastic

Utilisez la commande [Enable-EC2AddressTransfer](#).

Désactivation du transfert d'adresses IP Elastic

Cette section décrit comment désactiver un transfert d'adresses IP Elastic après que le transfert ait été activé.

Ces étapes doivent être effectuées par le compte source qui a activé le transfert.

Console

Pour désactiver un transfert d'adresse IP Elastic

1. Assurez-vous d'utiliser le AWS compte source.
2. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
3. Dans le panneau de navigation, choisissez Adresses IP Elastic.
4. Dans la liste des ressources des adresses IP Elastic, assurez-vous que la propriété qui affiche la colonne Transfer status (État du transfert) est activée.
5. Sélectionnez une ou plusieurs adresses IP Elastic dont Transfer status (État du transfert) est Pending (En attente), puis choisissez Actions, Disable transfer (Désactiver le transfert).
6. Confirmez en saisissant **disable** dans la zone de texte.
7. Sélectionnez Envoyer.

AWS CLI

Pour désactiver le transfert d'adresses IP Elastic

Utilisez la commande [disable-address-transfer](#).

PowerShell

Pour désactiver le transfert d'adresses IP Elastic

Utilisez la commande [Disable-EC2AddressTransfer](#).

Acceptation d'une adresse IP Elastic transférée

Cette section décrit comment accepter une adresse IP Elastic transférée.

Lorsque vous transférez une adresse IP Elastic, il existe une liaison en deux étapes entre les Comptes AWS. Lorsque le compte source lance le transfert, les comptes de transfert ont sept jours pour accepter le transfert de l'adresse IP Elastic. Pendant ces sept jours, le compte source peut consulter le transfert en attente (par exemple dans la AWS console ou à l'aide de la commande [AWS CLI describe-address-transfers](#)). Au bout de sept jours, le transfert expire et la propriété de l'adresse IP Elastic revient au compte source.

Lorsque vous acceptez des transferts, notez les exceptions suivantes qui peuvent se produire et comment les résoudre :

- **AddressLimitDépassé** : si votre compte de transfert a dépassé le quota d'adresses IP Elastic, le compte source peut activer le transfert d'adresses IP Elastic, mais cette exception se produit lorsque le compte de transfert essaie d'accepter le transfert. Par défaut, tous les AWS comptes sont limités à 5 adresses IP élastiques par région. Voir [Quota appliqué aux adresses IP Elastic](#) pour les instructions relatives à l'augmentation de la limite.
- **InvalidTransfer. AddressCustomPtrSet**: Si vous ou un membre de votre organisation avez configuré l'adresse IP élastique que vous essayez de transférer pour utiliser la recherche DNS inversée, le compte source peut activer le transfert pour l'adresse IP élastique, mais cette exception se produit lorsque le compte de transfert essaie d'accepter le transfert. Pour résoudre ce problème, le compte source doit supprimer l'enregistrement DNS de l'adresse IP Elastic. Pour plus d'informations, consultez [Utiliser des enregistrements DNS inverses pour les applications de messagerie](#).
- **InvalidTransfer. AddressAssociated**: Si une adresse IP élastique est associée à une instance ENI ou EC2, le compte source peut activer le transfert pour l'adresse IP élastique, mais cette exception se produit lorsque le compte de transfert essaie d'accepter le transfert. Pour résoudre ce problème, le compte source doit dissocier l'adresse IP Elastic. Pour plus d'informations, consultez [Dissocier une adresse IP Elastic](#).

Pour toute autre exception, [contactez AWS Support](#).

Cette procédure doit être suivie par le compte de transfert.

Console

Pour accepter un transfert d'adresse IP Elastic

1. Assurez-vous d'utiliser le compte de transfert.
2. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
3. Dans le panneau de navigation, choisissez Adresses IP Elastic.
4. Choisissez Actions, puis Accept transfer (Accepter le transfert).
5. Aucune balise associée à l'adresse IP Elastic transférée n'est transférée avec l'adresse IP Elastic lorsque vous acceptez le transfert. Si vous souhaitez définir une balise Name (Nom) pour l'adresse IP Elastic que vous acceptez, sélectionnez Create a tag with a key of 'Name' and a value that you specify (Créer une balise avec la clé « Nom » et une valeur que vous spécifiez).
6. Saisissez l'adresse IP Elastic que vous voulez transférer.
7. Si vous acceptez plusieurs adresses IP Elastic transférées, choisissez Add address (Ajouter une adresse) pour saisir une adresse IP Elastic supplémentaire.
8. Sélectionnez Envoyer.

AWS CLI

Pour accepter un transfert d'adresse IP Elastic

Utilisez la commande [accept-address-transfer](#).

PowerShell

Pour accepter un transfert d'adresse IP Elastic

Utilisez la commande [Approve-EC2AddressTransfer](#).

Libérer une adresse IP Elastic

Si vous n'avez plus besoin d'une adresse IP Elastic, nous vous recommandons de la libérer via l'une des méthodes suivantes. L'adresse à libérer ne doit pas être actuellement associée à une AWS ressource, telle qu'une instance EC2, une passerelle NAT ou un Network Load Balancer.

Note

Si vous avez contacté le AWS support pour configurer le DNS inversé pour une adresse IP élastique (EIP), vous pouvez supprimer le DNS inversé, mais vous ne pouvez pas libérer l'adresse IP élastique car elle a été verrouillée par le AWS support. Pour déverrouiller l'adresse IP élastique, contactez [AWS Support](#). Une fois l'adresse IP élastique déverrouillée, vous pouvez la libérer.

Console

Libérer une adresse IP Elastic

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic à libérer, puis choisissez Actions, Release Elastic IP addresses (Libérer des adresses IP Elastic).
4. Choisissez Release (Libérer).

AWS CLI

Libérer une adresse IP Elastic

Utilisez la commande [release-address](#) AWS CLI .

PowerShell

Libérer une adresse IP Elastic

Utilisez la [Remove-EC2Address](#) AWS Tools for Windows PowerShell commande.

Récupérer une adresse IP Elastic

Si vous avez libéré votre adresse IP Elastic, vous pouvez essayer de la récupérer. Les règles suivantes s'appliquent :

- Vous ne pouvez pas récupérer une adresse IP Elastic si celle-ci a été allouée à un autre compte AWS ou si cela risque d'entraîner un dépassement de votre limite d'adresses IP Elastic.
- Vous ne pouvez pas récupérer les balises associées à une adresse IP Elastic.

- Il n'est possible de récupérer une adresse IP Elastic qu'à l'aide de l'API Amazon EC2 ou d'un outil de ligne de commande.

AWS CLI

Pour récupérer une adresse IP Elastic

Utilisez la AWS CLI commande [allocate-address](#) et spécifiez l'adresse IP à l'aide du `--address` paramètre comme suit.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

PowerShell

Pour récupérer une adresse IP Elastic

Utilisez la [New-EC2Address](#) AWS Tools for Windows PowerShell commande et spécifiez l'adresse IP à l'aide du `-Address` paramètre comme suit.

```
PS C:\> New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

Utiliser des enregistrements DNS inverses pour les applications de messagerie

Si vous avez l'intention d'envoyer des e-mails à des tiers à partir d'une instance, nous vous recommandons de provisionner une ou plusieurs adresses IP Elastic et d'affecter des enregistrements DNS inversés statiques aux adresses IP Elastic que vous utilisez pour envoyer des e-mails. Cela peut vous aider à éviter que votre e-mail soit marqué comme spam par certaines organisations antispam. AWS travaille avec les fournisseurs de services Internet et les organisations antispam sur Internet afin de réduire le risque que les e-mails envoyés à partir de ces adresses soient marqués comme du spam.

Considérations

- Avant de créer un enregistrement DNS inverse, vous devez définir un enregistrement DNS de transfert correspondant (type d'enregistrement A) qui pointe vers votre adresse IP Elastic.
- Si un enregistrement DNS inverse est associé à une adresse IP Elastic, cette dernière est verrouillée pour votre compte et ne peut pas être libérée tant que l'enregistrement n'est pas supprimé.
- AWS GovCloud (US) Region

Vous ne pouvez pas créer d'enregistrement DNS inversé à l'aide de la console ou AWS CLI. AWS doit vous attribuer les enregistrements DNS inverses statiques. Accédez à la page [Request to remove reverse DNS and email sending limitations](#) (Demande de suppression des limitations DNS inversées et d'envoi d'e-mails) et renseignez vos adresses IP Elastic et vos enregistrements DNS inversés.

Créer un enregistrement DNS inverse

Pour créer un registre DNS inverse, choisissez l'onglet qui correspond à votre méthode préférée.

Console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic, puis choisissez Actions, Mettre à jour le DNS inverse.
4. Pour Reverse DNS domain name (Nom de domaine DNS inverse), saisissez le nom du domaine.
5. Saisissez **update** pour confirmer.
6. Sélectionnez Mise à jour.

AWS CLI

Utilisez la [modify-address-attribute](#) commande dans le AWS CLI, comme indiqué dans l'exemple suivant :

```
aws ec2 modify-address-attribute --allocation-id eipalloc-abcdef01234567890 --
domain-name example.com
{
  "Addresses": [
    {
      "PublicIp": "192.0.2.0",
      "AllocationId": "eipalloc-abcdef01234567890",
      "PtrRecord": "example.net."
      "PtrRecordUpdate": {
        "Value": "example.com.",
        "Status": "PENDING"
      }
    }
  ]
}
```

```
}
```

Supprimer un registre DNS inverse

Pour supprimer un registre DNS inverse, choisissez l'onglet qui correspond à votre méthode préférée.

Console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Adresses IP Elastic.
3. Sélectionnez l'adresse IP Elastic, puis choisissez Actions, Mettre à jour le DNS inverse.
4. Pour Reverse DNS domain name (Nom de domaine DNS inverse), effacez le nom du domaine.
5. Saisissez **update** pour confirmer.
6. Sélectionnez Mise à jour.

AWS CLI

Utilisez la [reset-address-attribute](#) commande dans le AWS CLI, comme indiqué dans l'exemple suivant :

```
aws ec2 reset-address-attribute --allocation-id eipalloc-abcdef01234567890 --  
attribute domain-name  
{  
  "Addresses": [  
    {  
      "PublicIp": "192.0.2.0",  
      "AllocationId": "eipalloc-abcdef01234567890",  
      "PtrRecord": "example.com."  
      "PtrRecordUpdate": {  
        "Value": "example.net.",  
        "Status": "PENDING"  
      }  
    }  
  ]  
}
```

Note

Si le message d'erreur suivant s'affiche lorsque vous exécutez la commande, vous pouvez envoyer une [demande de suppression des restrictions d'envoi d'e-mails](#) AWS Support pour obtenir de l'aide.

L'adresse comprenant l'identifiant d'allocation ne peut pas être lancée, car elle est verrouillée sur votre compte.

Quota appliqué aux adresses IP Elastic

Par défaut, tous les AWS comptes ont un quota de cinq (5) adresses IP élastiques par région, car les adresses Internet publiques (IPv4) sont une ressource publique rare. Nous vous encourageons vivement à utiliser une adresse IP Elastic principalement pour pouvoir remapper l'adresse à une autre instance dans le cas de la défaillance d'une instance et d'utiliser des [noms d'hôte DNS](#) pour toutes les autres communications internœuds.

Pour vérifier le nombre d'adresses IP Elastic utilisées

Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/> et choisissez Adresses IP Elastic dans le panneau de navigation.

Pour vérifier le quota actuel de votre compte pour les adresses IP Elastic

1. Ouvrez la console Service Quotas à l'adresse <https://console.aws.amazon.com/servicequotas/>.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez une région.
3. Sur le tableau de bord, choisissez Amazon Elastic Compute Cloud (Amazon EC2).

Si Amazon Elastic Compute Cloud (Amazon EC2) n'est pas répertorié dans le tableau de bord, choisissez services AWS , saisissez **EC2** dans le champ de recherche, puis choisissez Amazon Elastic Compute Cloud (Amazon EC2).

4. Sur la page des quotas du service Amazon EC2, entrez **IP** dans le champ de recherche. La limite est EC2-VPC Elastic IPs (Adresses IP Elastic EC2-VPC). Pour plus d'informations, choisissez la limite.

Si vous pensez que votre architecture justifie l'utilisation d'adresses IP Elastic supplémentaires, vous pouvez demander une augmentation de quota directement à partir de la console Service Quotas.

Pour demander l'augmentation d'un quota, choisissez [Demander une augmentation au niveau du compte](#). Pour plus d'informations, consultez [Quotas de service Amazon EC2](#).

Interfaces réseau Elastic

Une interface réseau Elastic est un composant réseau logique dans un VPC qui représente une carte réseau virtuelle. Elle peut inclure les attributs suivants :

- Une adresse IPv4 privée principale de la plage d'adresses IPv4 de votre VPC.
- Une adresse IPv6 principale de la plage d'adresses IPv6 de votre VPC.
- Une ou plusieurs adresses IPv4 privées secondaires de la plage d'adresses IPv4 de votre VPC.
- Une adresse IP Elastic (IPv4) par adresse IPv4 privée
- Une adresse IPv4 publique
- Une ou plusieurs adresses IPv6
- Un ou plusieurs groupes de sécurité
- Une adresse MAC
- Un indicateur de vérification origine/destination
- Une description

Vous pouvez créer et configurer des interfaces réseau et les attacher à des instances dans la même zone de disponibilité. Votre compte peut également comporter des interfaces réseau gérées par les demandeurs, qui sont créées et gérées par AWS des services pour vous permettre d'utiliser d'autres ressources et services. Vous ne pouvez pas gérer ces interfaces réseau vous-même. Pour plus d'informations, consultez [Interfaces réseau gérées par demandeur](#).

Cette AWS ressource est appelée interface réseau dans AWS Management Console et dans l'API Amazon EC2. Par conséquent, nous utilisons « interface réseau » dans cette documentation au lieu d'indiquer « interface réseau Elastic ». L'expression « interface réseau » dans cette documentation signifie toujours « interface réseau Elastic ».

Sommaire

- [Notions fondamentales concernant l'interface réseau](#)
- [Cartes réseau](#)
- [Adresses IP par interface réseau et par type d'instance](#)
- [Utiliser des interfaces réseau](#)

- [Meilleures pratiques pour la configuration des interfaces réseau](#)
- [Scénarios pour les interfaces réseau](#)
- [Interfaces réseau gérées par demandeur](#)
- [Attribuer des préfixes aux interfaces réseau Amazon EC2](#)

Notions fondamentales concernant l'interface réseau

Vous pouvez créer une interface réseau, l'attacher à une instance, la détacher d'une instance et l'attacher à une autre instance. Les attributs d'une interface réseau la suivent lorsque celle-ci est attachée à une instance ou détachée d'une instance, puis rattachée à une autre instance. Lorsque vous déplacez une interface réseau d'une instance vers une autre, le trafic réseau est redirigé vers la nouvelle instance.

Interface réseau principale

Chaque instance a une interface réseau par défaut, appelée l'interface réseau principale. Vous ne pouvez pas détacher une interface réseau principale d'une instance. Vous pouvez créer et attacher des Network Interfaces supplémentaires. Le nombre maximal d'interfaces réseau que vous pouvez utiliser varie en fonction du type d'instance. Pour plus d'informations, consultez [Adresses IP par interface réseau et par type d'instance](#).

Adresses IPv4 publiques pour les interfaces réseau

Dans un VPC, tous les sous-réseaux ont un attribut modifiable qui détermine si les interfaces réseau créées dans ce sous-réseau (et, par conséquent, les instances lancées dans ce sous-réseau) sont attribuées à une adresse IPv4 publique. Pour plus d'informations, consultez [Paramètres du sous-réseau](#) dans le Guide de l'utilisateur Amazon VPC. L'adresse IPv4 publique est attribuée à partir du pool d'adresses IPv4 publiques d'Amazon. Lorsque vous lancez une instance, l'adresse IP est attribuée à l'interface réseau principale qui est créée.

Lorsque vous créez une interface réseau, elle hérite l'attribut d'adressage IPv4 public du sous-réseau. Si vous modifiez par la suite l'attribut d'adressage IPv4 public du sous-réseau, l'interface réseau conserve le paramètre qui était en vigueur lorsqu'elle a été créée. Si vous lancez une instance et spécifiez une interface réseau existante comme interface réseau principale, l'attribut d'adresse IPv4 publique est déterminé par cette interface réseau.

Pour plus d'informations, consultez [Adresses IPv4 publiques](#).

Adresses IP Elastic pour l'interface réseau

Si vous disposez d'une adresse IP Elastic, vous pouvez l'associer à l'une des adresses IPv4 privées de l'interface réseau. Vous pouvez associer une adresse IP Elastic à chaque adresse IPv4 privée.

Si vous dissociez une adresse IP Elastic d'une interface réseau, vous pouvez la libérer dans le pool d'adresses. C'est la seule façon d'associer une adresse IP Elastic à une instance d'un sous-réseau ou d'un VPC différent, car les interfaces réseau sont spécifiques aux sous-réseaux.

Adresses IPv6 pour les interfaces réseau

Si vous associez des blocs d'adresse CIDR IPv6 à votre VPC et à votre sous-réseau, vous pouvez attribuer une ou plusieurs adresses IPv6 de la plage du sous-réseau à une interface réseau. Chaque adresse IPv6 peut être attribuée à une interface réseau.

Tous les sous-réseaux ont un attribut modifiable qui détermine si les interfaces réseau créées dans ce sous-réseau (et, par conséquent, les instances lancées dans ce sous-réseau) reçoivent automatiquement une adresse IPv6 de la plage du sous-réseau. Pour plus d'informations, consultez [Paramètres du sous-réseau](#) dans le Guide de l'utilisateur Amazon VPC. Lorsque vous lancez une instance, l'adresse IPv6 est attribuée à l'interface réseau principale qui est créée.

Pour plus d'informations, consultez [Adresses IPv6](#).

Délégation de préfixes

Un préfixe de délégation de préfixes est une plage CIDR IPv4 ou IPv6 privée réservée que vous allouez pour une attribution automatique ou manuelle aux interfaces réseau associées à une instance. En utilisant les préfixes délégués, vous pouvez lancer des services plus rapidement en attribuant une plage d'adresses IP sous la forme d'un préfixe unique.

Comportement de résiliation

Vous pouvez définir le comportement de résiliation d'une interface réseau attachée à une instance. Vous pouvez spécifier si l'interface réseau doit être supprimée automatiquement lorsque vous résiliez l'instance à laquelle celle-ci est attachée.

Vérification origine/destination

Vous pouvez activer ou désactiver les vérifications origine/destination, qui garantissent que l'instance est la source ou la destination du trafic qu'elle reçoit. Les vérifications origine/destination sont activées par défaut. Vous devez désactiver les vérifications origine/destination si l'instance exécute des services tels que la traduction d'adresses réseau, le routage ou les pare-feu.

Surveillance du trafic IP

Vous pouvez activer un journal de flux VPC sur votre interface réseau pour capturer des informations sur le trafic IP circulant vers et depuis l'interface réseau. Après avoir créé un journal de flux, vous pouvez consulter et récupérer ses données dans Amazon CloudWatch Logs. Pour plus d'informations, consultez la rubrique [Journaux de flux VPC](#) dans le Guide de l'utilisateur Amazon VPC.

Attribution automatique d'adresses IPv4 publiques

Vous pouvez activer et désactiver l'attribution automatique d'une adresse IPv4 publique à une interface réseau. Cette option peut être activée pour n'importe quelle interface réseau mais ne s'applique qu'à l'interface réseau principale (eth0). Pour plus d'informations, consultez [Gérer les adresses IP](#).

Cartes réseau

Les instances dotées de plusieurs cartes réseau offrent des performances réseau plus élevées, notamment des capacités de bande passante supérieure à 100 Gbit/s et des performances de débit de paquets accrues. Chaque interface réseau est connectée à une carte réseau. L'interface réseau principale doit être affectée à l'index de carte réseau 0.

Si vous activez Elastic Fabric Adapter (EFA) (EFA) lorsque vous lancez une instance prenant en charge plusieurs cartes réseau, toutes les cartes réseau sont disponibles. Vous pouvez attribuer un EFA maximum par carte réseau. Un EFA compte comme une interface réseau.

Les instances suivantes prennent en charge plusieurs cartes réseau. Tous les autres types d'instance prennent en charge une carte réseau.

Type d'instance	Nombre de cartes réseau
c6in.32xlarge	2
c6in.metal	2
d11.24xlarge	4
hpc6id.32xlarge	2
hpc7a.12xlarge	2
hpc7a.24xlarge	2

Type d'instance	Nombre de cartes réseau
hpc7a.48xlarge	2
hpc7a.96xlarge	2
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2
p4d.24xlarge	4
p4de.24xlarge	4
p5.48xlarge	32
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8
trn1n.32xlarge	16
u7in-16tb.224xlarge	2
u7in-24tb.224xlarge	2
u7in-32tb.224xlarge	2

Adresses IP par interface réseau et par type d'instance

Chaque type d'instance prend en charge un nombre maximum d'interfaces réseau, un nombre maximum d'adresses IPv4 privées par interface réseau et un nombre maximum d'adresses IPv6 par interface réseau. La limite pour les adresses IPv6 est distincte de la limite pour les adresses IPv4 privées par interface réseau. Certains types d'instance ne prennent pas en charge l'adressage IPv6.

Interfaces réseau disponibles

Le guide des types d'instances Amazon EC2 fournit des informations sur les interfaces réseau disponibles pour chaque type d'instance. Pour plus d'informations, consultez les ressources suivantes :

- [Spécifications du réseau — Usage général](#)
- [Spécifications du réseau — Optimisé pour le calcul](#)
- [Spécifications du réseau — Mémoire optimisée](#)
- [Spécifications du réseau — Stockage optimisé](#)
- [Spécifications du réseau — Calcul accéléré](#)
- [Spécifications du réseau — Calcul à haute performance](#)
- [Spécifications du réseau — Génération précédente](#)

Pour récupérer les informations d'interface réseau à l'aide du AWS CLI

Vous pouvez utiliser la AWS CLI commande [describe-instance-types](#) pour afficher des informations sur un type d'instance, telles que les interfaces réseau prises en charge et les adresses IP par interface. L'exemple suivant affiche ces informations pour toutes les instances C5.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*" --query
"InstanceTypes[].{Type: InstanceType, MaxENI: NetworkInfo.MaximumNetworkInterfaces,
IPv4addr: NetworkInfo.Ipv4AddressesPerInterface}" --output table
```

```
-----
|           DescribeInstanceTypes           |
+-----+-----+-----+
| IPv4addr | MaxENI |      Type      |
+-----+-----+-----+
|   30     |   8    | c5.4xlarge     |
|   50     |  15   | c5.24xlarge    |
|   15     |   4    | c5.xlarge      |
+-----+-----+-----+
```

30	8	c5.12xlarge	
10	3	c5.large	
15	4	c5.2xlarge	
50	15	c5.metal	
30	8	c5.9xlarge	
50	15	c5.18xlarge	
+-----+	+-----+	+-----+	+-----+

Utiliser des interfaces réseau

Vous pouvez travailler avec les interfaces réseau à l'aide de la console Amazon EC2 ou de la ligne de commande.

Sommaire

- [Créer une interface réseau](#)
- [Afficher les détails relatifs à une interface réseau](#)
- [Attacher une interface réseau à une instance](#)
- [Détacher une interface réseau d'une instance](#)
- [Gérer les adresses IP](#)
- [Modifier les attributs d'interface réseau](#)
- [Ajouter ou modifier des balises](#)
- [Supprimer une interface réseau](#)

Créer une interface réseau

Vous pouvez créer une interface réseau dans un sous-réseau. Une fois l'interface réseau créée, vous ne pouvez pas la déplacer vers un autre sous-réseau. Vous devez attacher une interface réseau à une instance dans la même zone de disponibilité.

Pour créer une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Sélectionnez Create network interface (Créer une interface réseau).
4. Sous Description, saisissez un nom descriptif.

5. Pour Sous-réseau (subnet), sélectionnez un sous-réseau. Les options disponibles dans les étapes suivantes varient en fonction du type de sous-réseau que vous sélectionnez (exclusivement IPv4, exclusivement IPv6 ou double pile (IPv4 et IPv6)).
6. Sous Private IPv4 address (Adresse IPv4 privée), effectuez l'une des actions suivantes :
 - Sélectionnez Auto-assign (Affectation automatique) pour permettre à Amazon EC2 de sélectionner une adresse IPv4 dans le sous-réseau.
 - Sélectionnez Custom (Personnalisé) et saisissez une adresse IPv4 que vous sélectionnez dans le sous-réseau.
7. (Pour les sous-réseaux avec adresses IPv6 uniquement) Sous IPv6 address (Adresse IPv6), effectuez l'une des opérations suivantes :
 - Sélectionnez None (Aucune) si vous ne souhaitez pas attribuer d'adresse IPv6 à l'interface réseau.
 - Sélectionnez Auto-assign (Affectation automatique) pour permettre à Amazon EC2 de sélectionner une adresse IPv6 dans le sous-réseau.
 - Sélectionnez Custom (Personnalisé) et saisissez une adresse IPv6 que vous sélectionnez dans le sous-réseau.
8. (Facultatif) Si vous créez une interface réseau dans un sous-réseau à double pile ou uniquement IPv6, vous avez la possibilité d'Attribuer une adresse IP IPv6 principale. Cela affecte une adresse IPv6 Global Unicast (GUA) principale à l'interface réseau. L'attribution d'une adresse IPv6 principale vous permet d'éviter de perturber le trafic vers les instances ou les ENI. Choisissez Enable si l'instance à laquelle cette ENI sera attachée repose sur le fait que son adresse IPv6 ne change pas. AWS attribuera automatiquement une adresse IPv6 associée à l'ENI attachée à votre instance comme adresse IPv6 principale. Une fois que vous avez activé une adresse GUA IPv6 comme adresse IPv6 principale, vous ne pouvez pas la désactiver. Lorsque vous activez une adresse GUA IPv6 comme adresse IPv6 principale, la première GUA IPv6 devient l'adresse IPv6 principale jusqu'à ce que l'instance soit résiliée ou que l'interface réseau soit détachée. Si plusieurs adresses IPv6 sont associées à une ENI attachée à votre instance et que vous activez une adresse IPv6 principale, la première adresse GUA IPv6 associée à l'ENI devient l'adresse IPv6 principale.
9. (Facultatif) Pour créer un Elastic Fabric Adapter (EFA), sélectionnez Elastic Fabric Adapter (EFA), puis Enable (Activer).
10. (Facultatif) Sous Paramètres avancés, pour Délai de suivi d'inactivité de la connexion, modifiez les délais d'inactivité de la connexion par défaut. Pour plus d'informations sur ces options, consultez [Délai de suivi d'inactivité de la connexion](#).

- Délai TCP établi : délai d'expiration (en secondes) pour les connexions TCP inactives dans un état établi. Min. : 60 secondes. Max. : 432 000 secondes (5 jours). Par défaut : 432 000 secondes. Recommandé : moins de 432 000 secondes.
 - Délai UDP : délai d'expiration (en secondes) pour les flux UDP inactifs qui n'ont vu du trafic que dans une seule direction ou une seule transaction requête-réponse. Min. : 30 secondes. Max. : 60 secondes. Par défaut : 30 secondes.
 - Délai d'expiration des flux UDP : délai d'expiration (en secondes) des flux UDP inactifs classés comme des flux ayant reçu plus d'une transaction requête-réponse. Min. : 60 secondes. Max. : 180 secondes (3 minutes). Par défaut : 180 secondes.
11. Pour Groupes de sécurité, sélectionnez un ou plusieurs groupes de sécurité.
 12. (Facultatif) Pour chaque balise, sélectionnez Add new tag (Ajouter une nouvelle balise) et saisissez une clé de balise et une valeur de balise facultative.
 13. Sélectionnez Create network interface (Créer une interface réseau).

Pour créer une interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [create-network-interface](#) (AWS CLI)
- [New-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Afficher les détails relatifs à une interface réseau

Vous pouvez afficher toutes les interfaces réseau dans votre compte.

Pour décrire une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Pour afficher la page de détails d'une interface réseau, sélectionnez l'ID de l'interface réseau. Sinon, pour afficher les informations sans quitter la page des interfaces réseau, cochez la case correspondant à l'interface réseau.

Pour décrire une interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel [Accès à Amazon EC2](#).

- [describe-network-interfaces](#) (AWS CLI)
- [Get-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Pour décrire un attribut d'interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [describe-network-interface-attribute](#) (AWS CLI)
- [Get-EC2NetworkInterfaceAttribute](#) (AWS Tools for Windows PowerShell)

Attacher une interface réseau à une instance

Vous pouvez attacher une interface réseau à toute instance dans la même zone de disponibilité que l'interface réseau en utilisant la page Instances ou Interfaces réseau de la console Amazon EC2.

Vous pouvez également attacher des interfaces réseau existantes lorsque vous [lancez des instances](#).

Important

Pour les instances EC2 d'un sous-réseau exclusivement IPv6, si vous attachez une interface réseau secondaire à l'instance, le nom d'hôte DNS privé de la seconde interface réseau sera résolu à la première adresse IPv6 de la première interface réseau de l'instance. Pour plus d'informations sur les noms d'hôte DNS privés d'instance EC2, consultez [Types de noms d'hôtes des instances Amazon EC2](#).

Si l'adresse IPv4 publique de votre instance est libérée, elle n'en reçoit pas de nouvelle si plusieurs interfaces réseau sont attachées à l'instance. Pour plus d'informations sur le comportement des adresses IPv4 publiques, consultez [Adresses IPv4 publiques](#).

Instances page

Pour attacher une interface réseau à une instance à l'aide de la page Instances

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Cochez la case correspondant à l'instance.
4. Sélectionnez Actions, Mise en réseau, Attacher l'interface réseau.
5. Choisissez un VPC. Si vous attachez une interface réseau secondaire à l'instance, celle-ci peut résider dans le même VPC que votre instance ou dans un VPC différent que vous possédez (à condition que l'interface réseau se trouve dans un sous-réseau situé dans la même zone de disponibilité que votre instance). Cela vous permet de créer des instances multi-résidents entre des VPC dotés de différentes configurations réseau et de sécurité.
6. Sélectionnez une interface réseau. Si l'instance prend en charge plusieurs cartes réseau, vous pouvez choisir une carte réseau.
7. Choisissez Attacher.

Network Interfaces page

Pour attacher une interface réseau à une instance à l'aide de la page Interfaces réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, puis Attach (Attacher).
5. Choisissez un type d'instance. Si l'instance prend en charge plusieurs cartes réseau, vous pouvez choisir une carte réseau.
6. Choisissez Attacher.

Pour attacher une interface réseau à une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel [Accès à Amazon EC2](#).

Note

Vous pouvez associer une interface réseau située dans un autre VPC (mais dans la même zone de disponibilité) à une instance à l'aide de la commande [AWS CLI `attach-network-interface`](#). Vous ne pouvez pas le faire en utilisant le AWS Management Console.

- [attach-network-interface](#) (AWS CLI)
- [Add-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Détacher une interface réseau d'une instance

Vous pouvez détacher une interface réseau secondaire à tout moment en utilisant la page Instances ou Interfaces réseau de la console Amazon EC2.

Si vous essayez de détacher une interface réseau attachée à une ressource d'un autre service, tel qu'un équilibreur de charge Elastic Load Balancing, une fonction Lambda, une passerelle ou une passerelle NAT WorkSpace, vous obtenez un message d'erreur indiquant que vous n'êtes pas autorisé à accéder à la ressource. Pour trouver quel service a créé la ressource attachée à une interface réseau, consultez la description de celle-ci. Si vous supprimez la ressource, son interface réseau est supprimée.

Instances page

Pour détacher une interface réseau d'une instance à l'aide de la page instances

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Cochez la case correspondant à l'instance. Consultez la section Network interfaces (Interfaces réseau) de l'onglet Networking (Mise en réseau) pour vérifier que l'interface réseau est attachée à une instance en tant qu'interface réseau secondaire.
4. Sélectionnez Actions, Mise en réseau, Détacher l'interface réseau.
5. Sélectionnez l'interface réseau, puis choisissez Détacher.

Network Interfaces page

Pour détacher une interface réseau d'une instance à l'aide de la page Interfaces réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau. Consultez la section Instance details (Détails de l'instance) de la Details (Détails) pour vérifier que l'interface réseau est attachée à une instance en tant qu'interface réseau secondaire.
4. Sélectionnez Actions, Detach (Détacher).
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Detach.
6. Si vous ne parvenez pas à détacher l'interface réseau de l'instance, choisissez Force detachment (Forcer le détachement), Enable (Activer), puis réessayez. Nous recommandons de ne forcer le détachement qu'en dernier recours. Forcer un détachement peut vous empêcher d'attacher une interface réseau différente sur le même index jusqu'à ce que vous redémarriez l'instance. Cela peut également empêcher les métadonnées de l'instance de refléter que l'interface réseau a été détachée jusqu'à ce que vous redémarriez l'instance.

Pour détacher une interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [detach-network-interface](#) (AWS CLI)
- [Dismount-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Gérer les adresses IP

Vous pouvez gérer les adresses IP suivantes pour vos interfaces réseau :

- Adresses IP Elastic (une par adresse IPv4 privée)
- Adresses IPv4
- Adresses IPv6
- Adresse IPv6 principale

Pour gérer les adresses IP Elastic d'une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Pour associer une adresse IP Elastic, procédez comme suit :
 - a. Sélectionnez Actions, Associate Address (Associer une adresse).
 - b. Sous Elastic IP address (Adresse IP Elastic), sélectionnez l'adresse IP Elastic.
 - c. Sous Private IPv4 address (Adresse IPv4 privée), sélectionnez l'adresse IPv4 privée à associer à l'adresse IP Elastic.
 - d. (Facultatif) Sélectionnez Allow the Elastic IP address to be reassociated (Autoriser la réassociation de l'adresse IP Elastic) si l'interface réseau est actuellement associée à une autre instance ou interface réseau.
 - e. Choisissez Associate.
5. Pour dissocier une adresse IP Elastic, procédez comme suit :
 - a. Choisissez Actions, Disassociate address.
 - b. Sous Public IP address (Adresse IP publique), sélectionnez l'adresse IP Elastic.
 - c. Choisissez Dissocier.

Pour gérer les adresses IPv4 et IPv6 d'une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Sélectionnez l'interface réseau.
4. Sélectionnez Actions, Manage IP addresses (Gérer les adresses IP).
5. Sélectionnez l'interface réseau.
6. Sous IPv4 Addresses (Adresses IPv4), modifiez les adresses IP selon vos besoins. Pour attribuer une adresse IPv4, choisissez Attribuer une nouvelle adresse IP, puis spécifiez une adresse IPv4 dans la plage de sous-réseaux ou laissez-en une pour AWS vous. Pour annuler l'attribution d'une adresse IPv4, choisissez Unassign (Annuler l'attribution) en regard de l'adresse.

7. Pour attribuer ou annuler l'attribution d'une adresse IPv4 publique à une interface réseau, choisissez Attribuer automatiquement une adresse IP publique. Cette option peut être activée ou désactivée pour n'importe quelle interface réseau, mais elle ne s'applique qu'à l'interface réseau principale (eth0).
8. Sous IPv6 Addresses (Adresses IPv6), modifiez les adresses IP selon vos besoins. Pour attribuer une adresse IPv6, choisissez Attribuer une nouvelle adresse IP, puis spécifiez une adresse IPv6 dans la plage de sous-réseaux ou AWS laissez-en une pour vous. Pour annuler l'attribution d'une adresse IPv6, choisissez Unassign (Annuler l'attribution) en regard de l'adresse.
9. (Facultatif) Si vous modifiez une interface réseau dans un sous-réseau à double pile ou uniquement IPv6, vous avez la possibilité d'Attribuer une adresse IP IPv6 principale. L'attribution d'une adresse IPv6 principale vous permet d'éviter de perturber le trafic vers les instances ou les ENI. Choisissez Enable si l'instance à laquelle cette ENI sera attachée repose sur le fait que son adresse IPv6 ne change pas. AWS attribuera automatiquement une adresse IPv6 associée à l'ENI attachée à votre instance comme adresse IPv6 principale. Une fois que vous avez activé une adresse GUA IPv6 comme adresse IPv6 principale, vous ne pouvez pas la désactiver. Lorsque vous activez une adresse GUA IPv6 comme adresse IPv6 principale, la première GUA IPv6 devient l'adresse IPv6 principale jusqu'à ce que l'instance soit résiliée ou que l'interface réseau soit détachée. Si plusieurs adresses IPv6 sont associées à une ENI attachée à votre instance et que vous activez une adresse IPv6 principale, la première adresse GUA IPv6 associée à l'ENI devient l'adresse IPv6 principale.
10. Choisissez Enregistrer.

Pour gérer les adresses IP d'une interface réseau à l'aide du AWS CLI

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [assign-ipv6-addresses](#)
- [associate-address](#)
- [disassociate-address](#)
- [unassign-ipv6-addresses](#)

Pour gérer les adresses IP d'une interface réseau à l'aide des outils pour Windows PowerShell

Vous pouvez utiliser l'une des commandes suivantes.

- [Register-EC2Address](#)
- [Register-EC2Ipv6 AddressList](#)
- [Unregister-EC2Address](#)
- [Unregister-EC2Ipv6 AddressList](#)

Modifier les attributs d'interface réseau

Vous pouvez modifier les attributs d'interface réseau suivants :

- [Description](#)
- [Groupes de sécurité](#)
- [Supprimer à la résiliation](#)
- [Vérification origine/destination](#)

Pour changer la description d'une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, Change description (Modifier la description).
5. Dans Description, saisissez une description de l'interface réseau.
6. Choisissez Enregistrer.

Pour changer les groupes de sécurité d'une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, Change security groups (Modifier les groupes de sécurité).
5. Pour Change Security Groups (Modifier les groupes de sécurité), sélectionnez les groupes de sécurité à utiliser, puis sélectionnez Save (Enregistrer).

Le groupe de sécurité et l'interface réseau doivent être créés pour le même VPC. Pour modifier le groupe de sécurité pour les interfaces appartenant à d'autres services, par exemple Elastic Load Balancing, faites-le via ce service.

Pour modifier le comportement de résiliation d'une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, Change termination behavior (Modifier le comportement de résiliation).
5. Sélectionner ou désactiver Delete on termination (Supprimer à la résiliation), Enable (Activer) au besoin, puis sélectionnez Save (Enregistrer).

Pour changer la vérification origine/destination d'une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sélectionnez Actions, Change source/dest check (Modifier la vérification source/dest).
5. Sélectionnez ou désactivez Source/destination check (Vérification origine/destination), Enable (Activer) au besoin, puis sélectionnez Save (Enregistrer).

Pour modifier les délais de suivi d'inactivité de la connexion :

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Choisissez Actions, Modifier le délai de la connexion.
5. Modifiez les délais de suivi d'inactivité de la connexion. Pour plus d'informations sur ces options, consultez [Délai de suivi d'inactivité de la connexion](#).

- Délai TCP établi : délai d'expiration (en secondes) pour les connexions TCP inactives dans un état établi. Min. : 60 secondes. Max. : 432 000 secondes (5 jours). Par défaut : 432 000 secondes. Recommandé : moins de 432 000 secondes.
- Délai UDP : délai d'expiration (en secondes) pour les flux UDP inactifs qui n'ont vu du trafic que dans une seule direction ou une seule transaction requête-réponse. Min. : 30 secondes. Max. : 60 secondes. Par défaut : 30 secondes.
- Délai d'expiration des flux UDP : délai d'expiration (en secondes) des flux UDP inactifs classés comme des flux ayant reçu plus d'une transaction requête-réponse. Min. : 60 secondes. Max. : 180 secondes (3 minutes). Par défaut : 180 secondes.

6. Choisissez Enregistrer.

Pour modifier les attributs d'interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (AWS Tools for Windows PowerShell)

Ajouter ou modifier des balises

Les balises sont les métadonnées que vous pouvez ajouter à une interface réseau. Les balises sont privées et sont uniquement visibles pour votre compte. Chaque balise est constituée d'une clé et d'une valeur facultative. Pour en savoir plus sur les identifications, consultez [Baliser vos ressources Amazon EC2](#).

Pour ajouter ou changer des balises pour une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau.
4. Sous l'onglet Tags (Balises), sélectionnez Manage tags (Gérer les balises).
5. Pour chaque balise à créer, sélectionnez Add new tag (Ajouter une nouvelle balise) et saisissez une clé et une valeur facultative. Lorsque vous avez terminé, sélectionnez Save.

Pour ajouter ou changer des balises pour une interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)

Supprimer une interface réseau

La suppression d'une interface réseau libère tous les attributs qui lui sont associés, ainsi que toute adresse IP privée ou adresse IP Elastic à utiliser par une autre instance.

Vous ne pouvez pas supprimer une interface réseau utilisée. Tout d'abord, vous devez [détacher l'interface réseau](#).

Pour supprimer une interface réseau à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Cochez la case correspondant à l'interface réseau, puis sélectionnez Actions, Delete (Supprimer).
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour supprimer une interface réseau à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [delete-network-interface](#) (AWS CLI)
- [Remove-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Meilleures pratiques pour la configuration des interfaces réseau

- Vous pouvez attacher une interface réseau à une instance lorsqu'elle est en cours d'exécution (attachement de secours), arrêtée (attachement à chaud) ou en cours de lancement (attachement à froid).

- Vous pouvez détacher les interfaces réseau secondaires lorsque l'instance s'exécute ou est arrêtée. Toutefois, vous ne pouvez pas détacher l'interface réseau principale.
- Vous pouvez déplacer une interface réseau secondaire d'une instance à une autre si les instances sont dans la même zone de disponibilité et le même VPC, mais dans des sous-réseaux différents.
- Lors du lancement d'une instance à l'aide de la CLI, de l'API ou d'un kit SDK, vous pouvez spécifier l'interface réseau principale et des interfaces réseau supplémentaires.
- Le lancement d'une instance Amazon Linux ou Windows Server avec plusieurs interfaces réseau configure automatiquement les interfaces, les adresses IPv4 privées et les tables de routage du système d'exploitation de l'instance.
- Un attachement à chaud ou de secours d'une interface réseau supplémentaire peut nécessiter que vous mettiez en place manuellement la deuxième interface, configurez l'adresse IPv4 privée et modifiez la table de routage en conséquence. Les instances qui exécutent Amazon Linux ou Windows Server reconnaissent automatiquement l'attachement à chaud ou de secours et se configurent elles-mêmes.
- Vous ne pouvez pas attacher une autre interface réseau à une instance (par exemple, une configuration d'association de cartes réseau) pour augmenter ou doubler la bande passante réseau vers ou depuis l'instance à deux interfaces réseau.
- Si vous attachez plusieurs interfaces réseau du même sous-réseau à une instance, vous pouvez être confronté à des problèmes de mise en réseau comme le routage asymétrique. Si possible, utilisez plutôt une adresse IPv4 privée secondaire sur l'interface réseau principale.
- Instances Windows : si vous utilisez plusieurs interfaces réseau, vous devez configurer les interfaces réseau pour utiliser le routage statique.

Configurer votre interface réseau à l'aide de `ec2-net-utils` pour Amazon Linux 2

Note

Pour AL2023, le package `amazon-ec2-net-utils` génère des configurations spécifiques à l'interface dans le répertoire `/run/systemd/network`. Pour plus d'informations, consultez la rubrique [Networking service](#) du Guide de l'utilisateur Amazon Linux 2023.

Les AMI Amazon Linux 2 peuvent contenir des scripts supplémentaires installés par AWS, appelés `ec2-net-utils`. Ces scripts automatisent le cas échéant la configuration de vos interfaces réseau. Ces scripts sont disponibles pour Amazon Linux 2 uniquement.

Utilisez la commande suivante pour installer le package sur Amazon Linux 2 s'il n'est pas déjà installé, ou mettez-le à jour s'il est installé et que des mises à jour supplémentaires sont disponibles :

```
$ yum install ec2-net-utils
```

Les composants suivants font partie de `ec2-net-utils` :

`udev rules (/etc/udev/rules.d)`

Identifie les interfaces réseau qui sont attachées, détachées ou rattachées à une instance en cours d'exécution, et s'assure que le script `hotplug` s'exécute (`53-ec2-network-interfaces.rules`). Mappe l'adresse MAC sur un nom de périphérique (`75-persistent-net-generator.rules`, qui génère `70-persistent-net.rules`).

`script hotplug`

Génère un fichier de configuration d'interface adapté à une utilisation avec DHCP (`/etc/sysconfig/network-scripts/ifcfg-ethN`). Génère également un fichier de configuration de route (`/etc/sysconfig/network-scripts/route-ethN`).

`script DHCP`

Chaque fois qu'une Network Interface reçoit un nouveau bail DHCP, ce script interroge les métadonnées d'instance pour des adresses IP Elastic. Pour chaque adresse IP Elastic, il ajoute une règle à la base de données de politiques de routage pour s'assurer que le trafic sortant à partir de cette adresse utilise l'interface réseau correcte. Il ajoute également chaque adresse IP privée à l'interface réseau comme adresse secondaire.

`ec2ifup ethN (/usr/sbin/)`

Étend la fonctionnalité de la commande standard `ifup`. Une fois que ce script a réécrit les fichiers de configuration `ifcfg-ethN` et `route-ethN`, il exécute `ifup`.

`ec2ifdown ethN (/usr/sbin/)`

Étend la fonctionnalité de la commande standard `ifdown`. Une fois que le script a supprimé les règles pour l'interface réseau de la base de données des stratégies de routage, il exécute `ifdown`.

`ec2ifscan (/usr/sbin/)`

Recherche les interfaces réseau qui n'ont pas été configurées et les configure.

Ce script n'est pas disponible dans la version initiale de `ec2-net-utils`.

Pour répertorier les fichiers de configuration générés par `ec2-net-utils`, utilisez la commande suivante :

```
$ ls -l /etc/sysconfig/network-scripts/*-eth?
```

Pour désactiver l'automatisation, vous pouvez ajouter `EC2SYNC=no` au fichier `ifcfg-ethN` correspondant. Par exemple, utilisez la commande suivante pour désactiver l'automatisation pour l'interface `eth1` :

```
$ sed -i -e 's/^EC2SYNC=yes/EC2SYNC=no/' /etc/sysconfig/network-scripts/ifcfg-eth1
```

Pour désactiver complètement l'automatisation, vous pouvez supprimer le package à l'aide de la commande suivante :

```
$ yum remove ec2-net-utils
```

Scénarios pour les interfaces réseau

Il peut être utile d'attacher plusieurs Network Interfaces à une instance si vous souhaitez :

- créer un réseau de gestion ;
- Utilisez des composants réseau et de sécurité dans votre cloud privé virtuel (VPC).
- créer des instances à deux interfaces réseau avec des charges de travail/rôles sur des sous-réseaux distincts ;
- créer une solution haute disponibilité à faible coût.

Créer un réseau de gestion

Ce scénario décrit comment créer un réseau de gestion doté d'interfaces réseau, en fonction des critères et paramètres suivants (image ci-dessous).

Critères

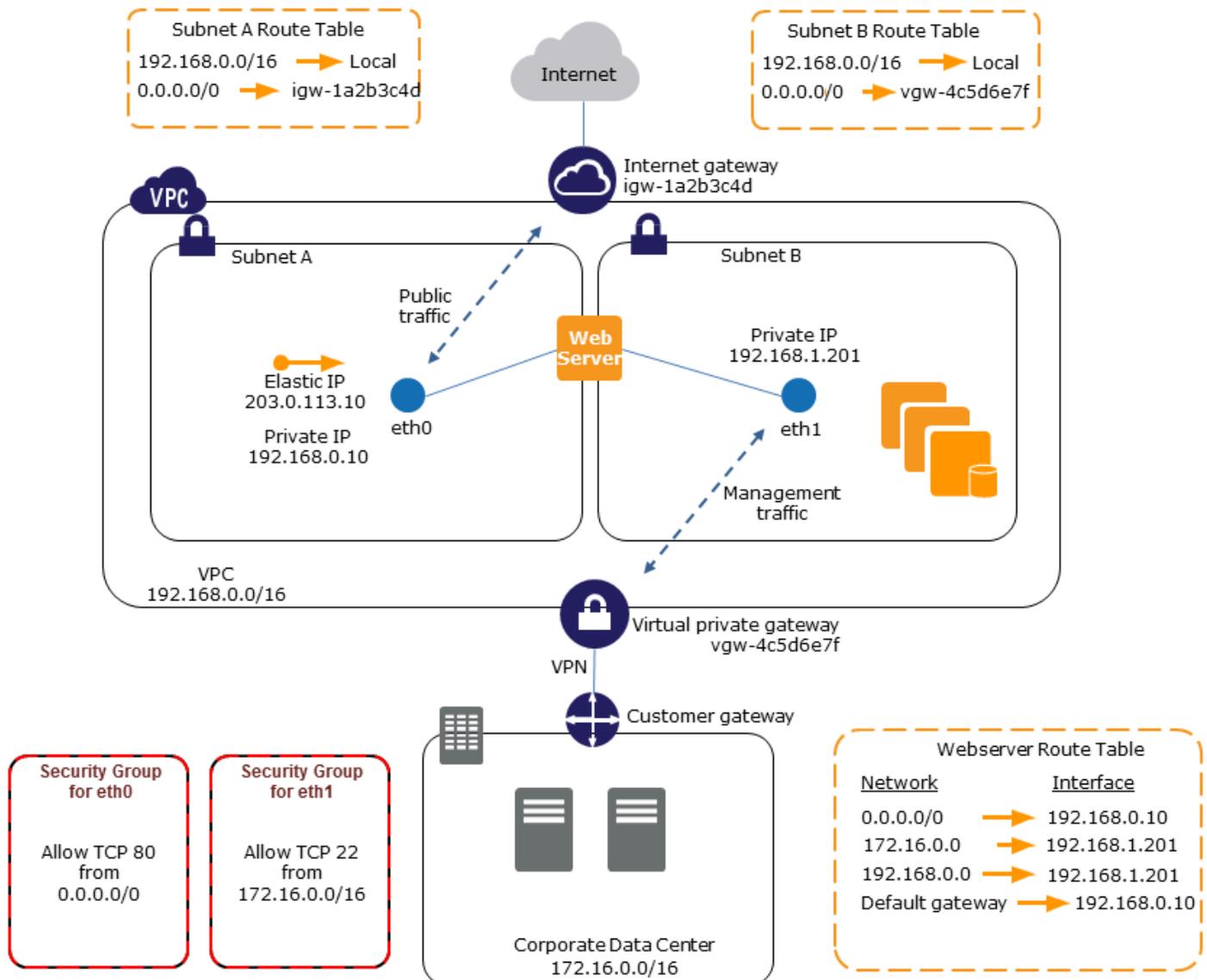
- L'interface réseau principale sur l'instance (`eth0`) gère le trafic public.
- L'interface réseau secondaire sur l'instance (`eth1`) gère le trafic de gestion du backend. Elle est connectée à un sous-réseau distinct qui dispose de contrôles d'accès plus restrictifs et se trouve dans la même zone de disponibilité (AZ) que l'interface réseau principale.

Paramètres

- L'interface réseau principale, qui peut ou non se trouver derrière un équilibreur de charge, a un groupe de sécurité associé qui autorise l'accès au serveur à partir d'Internet. Par exemple, autoriser les ports TCP 80 et 443 depuis `0.0.0.0/0` ou depuis l'équilibreur de charge.
- L'interface réseau secondaire possède un groupe de sécurité associé qui autorise uniquement l'accès SSH, initié depuis l'un des emplacements suivants :
 - Une plage autorisée d'adresses IP, soit au sein du VPC, soit depuis Internet.
 - Sous-réseau privé au sein de la même zone de disponibilité que l'interface réseau principale.
 - Passerelle privée virtuelle.

Note

Pour assurer les fonctions de basculement, pensez à utiliser une adresse IPv4 privée secondaire pour le trafic entrant sur une interface réseau. Dans le cas de la défaillance d'une instance, vous pouvez déplacer l'interface et/ou l'adresse IPv4 privée secondaire vers une instance de secours.



Utilisation de composants de réseau et de sécurité dans votre VPC

Certains composants de réseau et de sécurité tiers, tels que des équilibreurs de charge, des serveurs NAT (Network Address Translation, traduction d'adresses réseau) et des serveurs proxy, doivent, de préférence, être configurés avec plusieurs Network Interfaces. Vous pouvez créer et attacher des interfaces réseau secondaires à des instances qui exécutent ces types d'applications, et configurer les interfaces supplémentaires avec leurs propres adresses IP publiques et privées, groupes de sécurité et vérification origine/destination.

Création d'instances à deux interfaces réseau avec des charges de travail/rôles sur des sous-réseaux distincts

Vous pouvez placer une interface réseau sur chacun de vos serveurs web qui se connecte à un réseau de niveau intermédiaire où réside un serveur d'applications. Le serveur d'applications peut également avoir deux interfaces réseau sur le réseau backend (sous-réseau) où réside le serveur de base de données. Au lieu d'acheminer des paquets réseau via les instances à deux interfaces réseau, chaque instance à deux interfaces réseau reçoit et traite les demandes sur le serveur frontal, établit une connexion au serveur backend, puis envoie les demandes aux serveurs se trouvant sur le réseau backend.

Création d'instances à deux interfaces réseau avec des charges de travail/rôles sur des VPC distincts au sein du même compte

Vous pouvez lancer une instance EC2 dans un VPC et attacher une ENI secondaire d'un autre VPC (mais dans la même zone de disponibilité) à l'instance. Cela vous permet de créer des instances multi-résidents entre des VPC dotés de différentes configurations réseau et de sécurité. Vous ne pouvez pas créer d'instances multihébergées entre des VPC de différents comptes. AWS

Vous pouvez utiliser des instances à deux interfaces réseau entre des VPC dans les cas d'utilisation suivants :

- Contourner les chevauchements d'adresse CIDR lorsque l'appairage de deux VPC est impossible : vous pouvez tirer parti d'une adresse CIDR secondaire dans un VPC et autoriser une instance à communiquer entre deux plages d'adresses IP ne se chevauchant pas.
- Connecter plusieurs VPC au sein d'un même compte : activez la communication entre des ressources individuelles qui seraient normalement séparées par des limites de VPC.

Création d'une solution haute disponibilité à faible coût

Si l'une de vos instances remplissant une fonction particulière subit une défaillance, son Network Interface peut être attachée à une instance de remplacement ou de hot standby préconfigurée pour le même rôle afin de récupérer rapidement le service. Par exemple, vous pouvez utiliser une interface réseau comme interface réseau principale ou secondaire d'un service critique tel qu'une instance de base de données ou une instance NAT. Si une instance subit une défaillance, vous (ou, plus probablement, le code s'exécutant pour votre compte) pouvez attacher l'interface réseau à une instance de secours à chaud. Comme l'interface conserve ses adresses IP privées, ses adresses IP Elastic et son adresse MAC, le trafic réseau commence à passer vers l'instance de secours dès

que vous attachez l'interface réseau à l'instance de remplacement. Les utilisateurs rencontreront une brève perte de connectivité entre le moment où l'instance subit la défaillance et celui où l'interface réseau est attachée à l'instance de secours, mais aucune modification de la table de routage ou de votre serveur DNS n'est requise.

Interfaces réseau gérées par demandeur

Une interface réseau gérée par le demandeur est une interface réseau qu'un Service AWS crée dans votre VPC en votre nom. L'interface réseau est associée à une ressource pour un autre service, telle qu'une instance de base de données d'Amazon RDS, une passerelle NAT ou un point de terminaison d'un VPC d'interface de AWS PrivateLink.

Considérations

- Vous pouvez afficher les interfaces réseau gérées par demandeur dans votre compte. Vous pouvez ajouter ou supprimer des balises, mais vous ne pouvez pas modifier d'autres propriétés d'une interface réseau gérée par le demandeur.
- Vous ne pouvez pas détacher une interface réseau gérée par le demandeur.
- Lorsque vous supprimez la ressource associée à une interface réseau gérée par le demandeur, l'interface réseau Service AWS est détachée et supprimée. Si le service a détaché une interface réseau, mais ne l'a pas supprimée, vous pouvez supprimer l'interface réseau détachée.

Pour afficher les interfaces réseau gérées par demandeur à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Network & Security (Réseau et sécurité); Network Interfaces (Interfaces réseau).
3. Sélectionnez l'ID de l'interface réseau pour ouvrir sa page de détails.
4. Les principaux champs que vous pouvez utiliser pour déterminer l'objectif de l'interface réseau sont les suivants :
 - Description: description fournie par le service AWS ayant créé l'interface. Par exemple, « VPC Endpoint Interface vpce 089f2123488812123 ».
 - Géré par le demandeur : indique si l'interface réseau est gérée par AWS
 - ID du demandeur : alias ou identifiant de AWS compte du principal ou du service qui a créé l'interface réseau. Si vous avez créé l'interface réseau, il s'agit de votre Compte AWS identifiant. Sinon, un autre principal ou service l'a créé.

Pour afficher les interfaces réseau gérées par les demandeurs à l'aide du AWS CLI

Utilisez la commande [describe-network-interfaces](#) comme suit.

```
aws ec2 describe-network-interfaces --filters Name=requester-managed,Values=true
```

Voici un exemple de sortie montrant les principaux champs que vous pouvez utiliser pour déterminer l'objectif de l'interface réseau : `Description` et `InterfaceType`.

```
{
  ...
  "Description": "VPC Endpoint Interface vpce-089f2123488812123",
  ...
  "InterfaceType": "vpc_endpoint",
  ...
  "NetworkInterfaceId": "eni-0d11e3ccd2c0e6c57",
  ...
  "RequesterId": "727180483921",
  "RequesterManaged": true,
  ...
}
```

Pour afficher les interfaces réseau gérées par les demandeurs à l'aide des Outils pour Windows PowerShell

Utilisez l'[Get-EC2NetworkInterface](#) applet de commande comme suit.

```
Get-EC2NetworkInterface -Filter @{ Name="requester-managed"; Values="true" }
```

Voici un exemple de sortie montrant les principaux champs que vous pouvez utiliser pour déterminer l'objectif de l'interface réseau : `Description` et `InterfaceType`.

```
Description      : VPC Endpoint Interface vpce-089f2123488812123
...
InterfaceType    : vpc_endpoint
...
NetworkInterfaceId : eni-0d11e3ccd2c0e6c57
...
RequesterId      : 727180483921
RequesterManaged : True
```

...

Attribuer des préfixes aux interfaces réseau Amazon EC2

Vous pouvez attribuer une plage CIDR IPv4 ou IPv6 privée, automatiquement ou manuellement, à vos interfaces réseau. En attribuant des préfixes, vous mettez à l'échelle et simplifiez la gestion des applications, y compris les applications de conteneur et de réseau qui nécessitent plusieurs adresses IP sur une instance. Pour plus d'informations sur l'adressage IPv4 et IPv6, veuillez consulter la rubrique [Adressage IP des instances Amazon EC2](#).

Les options suivantes sont disponibles :

- Affectation automatique : AWS choisit le préfixe dans le bloc d'adresse CIDR IPv4 ou IPv6 de votre sous-réseau VPC et l'affecte à votre interface réseau.
- Affectation manuelle : vous spécifiez le préfixe à partir du bloc d'adresse CIDR IPv4 ou IPv6 de votre sous-réseau VPC AWS et vous vérifiez que le préfixe n'est pas déjà attribué à d'autres ressources avant de l'attribuer à votre interface réseau.

L'attribution de préfixes présente les avantages suivants :

- Augmentation du nombre d'adresses IP sur une interface réseau : lorsque vous utilisez un préfixe, vous attribuez un bloc d'adresses IP par opposition à des adresses IP individuelles. Cela accroît le nombre d'adresses IP d'une interface réseau.
- Gestion simplifiée des VPC pour les conteneurs : dans les applications de conteneur, chaque conteneur nécessite une adresse IP unique. L'attribution de préfixes à votre instance simplifie la gestion de vos VPC, car vous pouvez lancer et résilier des conteneurs sans avoir à appeler les API Amazon EC2 pour des attributions IP individuelles.

Table des matières

- [Notions de base pour l'attribution de préfixes](#)
- [Considérations et limites pour les préfixes](#)
- [Utilisation de préfixes](#)

Notions de base pour l'attribution de préfixes

- Vous pouvez attribuer un préfixe à des interfaces réseau nouvelles ou existantes.

- Pour utiliser des préfixes, vous devez attribuer un préfixe à votre interface réseau, puis attacher l'interface réseau à votre instance, puis configurer votre système d'exploitation.
- Lorsque vous choisissez de spécifier un préfixe, celui-ci doit répondre aux critères suivants :
 - Le préfixe IPv4 que vous pouvez spécifier est /28.
 - Le préfixe IPv6 que vous pouvez spécifier est /80.
 - Le préfixe se trouve dans le bloc d'adresses CIDR du sous-réseau de l'interface réseau et ne se chevauche pas avec d'autres préfixes ou adresses IP attribués aux ressources existantes dans le sous-réseau.
- Vous pouvez attribuer un préfixe à l'interface réseau principale ou secondaire.
- Vous pouvez attribuer une adresse IP Elastic à une interface réseau à laquelle un préfixe est attribué.
- Vous pouvez également attribuer une adresse IP Elastic à la partie adresse IP du préfixe attribué.
- Un nom d'hôte DNS privé (interne) est résolu en adresse IPv4 privée de l'instance.
- Nous attribuons chaque adresse IPv4 privée pour une interface réseau, notamment celles provenant de préfixes, à l'aide des formats suivants :
 - Région us-east-1

```
ip-private-ipv4-address.ec2.internal
```

- Toutes les autres régions

```
ip-private-ipv4-address.region.compute.internal
```

Considérations et limites pour les préfixes

Prenez en considération les points suivants lorsque vous utilisez des préfixes :

- Les interfaces réseau avec préfixes sont prises en charge avec [les instances créées sur le système AWS Nitro](#).
- Les préfixes pour les interfaces réseau sont limités aux adresses IPv6 et aux adresses IPv4 privées.
- Le nombre maximal d'adresses IP que vous pouvez attribuer à une interface réseau dépend du type d'instance. Chaque préfixe que vous attribuez à une interface réseau est considéré comme une adresse IP unique. Par exemple, une instance `c5.large` a une limite de 10 adresses IPv4 par interface réseau. Chaque interface réseau de cette instance possède une adresse IPv4

principale. Si une interface réseau ne possède pas d'adresses IPv4 secondaires, vous pouvez attribuer jusqu'à 9 préfixes à l'interface réseau. Pour chaque adresse IPv4 supplémentaire que vous attribuez à une interface réseau, vous pouvez attribuer un préfixe de moins à l'interface réseau. Pour plus d'informations, consultez [Adresses IP par interface réseau et par type d'instance](#).

- Les préfixes sont inclus dans les vérifications origine/destination.

Utilisation de préfixes

Vous pouvez utiliser des préfixes avec vos interfaces réseau comme suit.

Tâches

- [Attribuer des préfixes pendant la création de l'interface réseau](#)
- [Attribuer des préfixes aux interfaces réseau existantes](#)
- [Configurer votre système d'exploitation pour les interfaces réseau avec des préfixes](#)
- [Afficher les préfixes affectés à vos interfaces réseau](#)
- [Supprimer les préfixes de vos interfaces réseau](#)

Attribuer des préfixes pendant la création de l'interface réseau

Si vous utilisez l'option d'attribution automatique, vous pouvez réserver un bloc d'adresses IP dans votre sous-réseau. AWS choisit les préfixes de ce bloc. Pour plus d'informations, consultez [Subnet CIDR reservations](#) dans le Guide de l'utilisateur Amazon VPC.

Après avoir créé l'interface réseau, utilisez la AWS CLI commande [attach-network-interface pour associer l'interface](#) réseau à votre instance. Vous devez configurer votre système d'exploitation afin de prendre en charge les interfaces réseau avec des préfixes. Pour plus d'informations, consultez [Configurer votre système d'exploitation pour les interfaces réseau avec des préfixes](#).

Tâches

- [Attribuer des préfixes automatiques pendant la création de l'interface réseau](#)
- [Attribuer des préfixes spécifiques pendant la création de l'interface réseau](#)

Attribuer des préfixes automatiques pendant la création de l'interface réseau

Pour affecter des préfixes automatiques lors de la création de l'interface réseau utilisez l'une des méthodes suivantes.

Console

Pour affecter des préfixes automatiques lors de la création de l'interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Network Interfaces (Interfaces réseau), puis sélectionnez Create network interface (Créer une interface réseau).
3. Indiquez une description de l'interface réseau, sélectionnez le sous-réseau dans lequel vous souhaitez créer l'interface réseau et configurez les adresses privées IPv4 et IPv6.
4. Développez la section Advanced settings (Paramètres avancés) et procédez comme suit :
 - a. Pour affecter automatiquement un préfixe IPv4, sélectionnez Auto-assign (Affectation automatique) sous IPv4 prefix delegation (Délégation du préfixe IPv4). Ensuite, pour Number of IPv4 prefixes (Nombre de préfixes IPv4), indiquez le nombre de préfixes à affecter.
 - b. Pour affecter automatiquement un préfixe IPv6, sélectionnez Auto-assign (Affectation automatique) sous IPv6 prefix delegation (Délégation du préfixe IPv6). Ensuite, pour Number of IPv6 prefixes (Nombre de préfixes IPv6), indiquez le nombre de préfixes à affecter.

Note

L'option IPv6 prefix delegation (délégation du préfixe IPv6) s'affiche uniquement si le sous-réseau sélectionné est activé pour IPv6.

5. Sélectionnez les groupes de sécurité à associer à l'interface réseau et attribuez des balises de ressources si nécessaire.
6. Sélectionnez Create network interface (Créer une interface réseau).

AWS CLI

Pour attribuer des préfixes IPv4 automatiques lors de la création de l'interface réseau

Utilisez la [create-network-interface](#) commande et définissez `--ipv4-prefix-count` le nombre de préfixes que vous souhaitez AWS attribuer. Dans l'exemple suivant, AWS attribue un 1 préfixe.

```
$ C:\> aws ec2 create-network-interface \  
--subnet-id subnet-047cfed18eEXAMPLE \  
--ipv4-prefix-count 1
```

```
--description "IPv4 automatic example" \  
--ipv4-prefix-count 1
```

Exemple de sortie

```
{  
  "NetworkInterface": {  
    "AvailabilityZone": "us-west-2a",  
    "Description": "IPv4 automatic example",  
    "Groups": [  
      {  
        "GroupName": "default",  
        "GroupId": "sg-044c2de2c4EXAMPLE"  
      }  
    ],  
    "InterfaceType": "interface",  
    "Ipv6Addresses": [],  
    "MacAddress": "02:98:65:dd:18:47",  
    "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",  
    "OwnerId": "123456789012",  
    "PrivateIpAddress": "10.0.0.62",  
    "PrivateIpAddresses": [  
      {  
        "Primary": true,  
        "PrivateIpAddress": "10.0.0.62"  
      }  
    ],  
    "Ipv4Prefixes": [  
      {  
        "Ipv4Prefix": "10.0.0.208/28"  
      }  
    ],  
    "RequesterId": "AIDAIV5AJI5LXF5XXDPC0",  
    "RequesterManaged": false,  
    "SourceDestCheck": true,  
    "Status": "pending",  
    "SubnetId": "subnet-047cfed18eEXAMPLE",  
    "TagSet": [],  
    "VpcId": "vpc-0e12f52b21EXAMPLE"  
  }  
}
```

Pour attribuer des préfixes IPv6 automatiques lors de la création de l'interface réseau

Utilisez la [create-network-interface](#) commande et définissez `--ipv6-prefix-count` le nombre de préfixes que vous souhaitez AWS attribuer. Dans l'exemple suivant, AWS attribue un 1 préfixe.

```
$ C:\> aws ec2 create-network-interface \  
--subnet-id subnet-047cfed18eEXAMPLE \  
--description "IPv6 automatic example" \  
--ipv6-prefix-count 1
```

Exemple de sortie

```
{  
  "NetworkInterface": {  
    "AvailabilityZone": "us-west-2a",  
    "Description": "IPv6 automatic example",  
    "Groups": [  
      {  
        "GroupName": "default",  
        "GroupId": "sg-044c2de2c4EXAMPLE"  
      }  
    ],  
    "InterfaceType": "interface",  
    "Ipv6Addresses": [],  
    "MacAddress": "02:bb:e4:31:fe:09",  
    "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",  
    "OwnerId": "123456789012",  
    "PrivateIpAddress": "10.0.0.73",  
    "PrivateIpAddresses": [  
      {  
        "Primary": true,  
        "PrivateIpAddress": "10.0.0.73"  
      }  
    ],  
    "Ipv6Prefixes": [  
      {  
        "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"  
      }  
    ],  
    "RequesterId": "AIDAIV5AJI5LXF5XXDPC0",  
    "RequesterManaged": false,  
    "SourceDestCheck": true,  
    "Status": "pending",  
    "SubnetId": "subnet-047cfed18eEXAMPLE",  
    "TagSet": [],
```

```
    "VpcId": "vpc-0e12f52b21EXAMPLE"  
  }  
}
```

Attribuer des préfixes spécifiques pendant la création de l'interface réseau

Vous pouvez affecter des préfixes spécifiques lors de la création d'interface réseau à l'aide de l'une des méthodes suivantes.

Console

Pour affecter des préfixes spécifiques lors de la création de l'interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Network Interfaces (Interfaces réseau), puis sélectionnez Create network interface (Créer une interface réseau).
3. Indiquez une description de l'interface réseau, sélectionnez le sous-réseau dans lequel vous souhaitez créer l'interface réseau et configurez les adresses privées IPv4 et IPv6.
4. Développez la section Advanced settings (Paramètres avancés) et procédez comme suit :
 - a. Pour attribuer un préfixe IPv4 spécifique, sélectionnez Custom (Personnaliser) sous IPv4 prefix delegation (Délégation du préfixe IPv4). Puis sélectionnez Add new prefix (Ajouter un nouveau préfixe) et saisissez le préfixe à utiliser.
 - b. Pour attribuer un préfixe IPv6 spécifique, sélectionnez Custom (Personnaliser) sous IPv6 prefix delegation (Délégation du préfixe IPv6). Puis sélectionnez Add new prefix (Ajouter un nouveau préfixe) et saisissez le préfixe à utiliser.

Note

L'option IPv6 prefix delegation (délégation du préfixe IPv6) s'affiche uniquement si le sous-réseau sélectionné est activé pour IPv6.

5. Sélectionnez les groupes de sécurité à associer à l'interface réseau et attribuez des balises de ressources si nécessaire.
6. Sélectionnez Create network interface (Créer une interface réseau).

AWS CLI

Pour attribuer des préfixes IPv4 spécifiques lors de la création de l'interface réseau

Utilisez la [create-network-interface](#) commande et définissez `--ipv4-prefixes` les préfixes. AWS sélectionne les adresses IP dans cette plage. Dans l'exemple suivant, le préfixe CIDR est `10.0.0.208/28`.

```
$ C:\> aws ec2 create-network-interface \  
  --subnet-id subnet-047cfed18eEXAMPLE \  
  --description "IPv4 manual example" \  
  --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Exemple de sortie

```
{  
  "NetworkInterface": {  
    "AvailabilityZone": "us-west-2a",  
    "Description": "IPv4 manual example",  
    "Groups": [  
      {  
        "GroupName": "default",  
        "GroupId": "sg-044c2de2c4EXAMPLE"  
      }  
    ],  
    "InterfaceType": "interface",  
    "Ipv6Addresses": [],  
    "MacAddress": "02:98:65:dd:18:47",  
    "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",  
    "OwnerId": "123456789012",  
    "PrivateIpAddress": "10.0.0.62",  
    "PrivateIpAddresses": [  
      {  
        "Primary": true,  
        "PrivateIpAddress": "10.0.0.62"  
      }  
    ],  
    "Ipv4Prefixes": [  
      {  
        "Ipv4Prefix": "10.0.0.208/28"  
      }  
    ],  
    "RequesterId": "AIDAIV5AJI5LXF5XXDPC0",
```

```

    "RequesterManaged": false,
    "SourceDestCheck": true,
    "Status": "pending",
    "SubnetId": "subnet-047cfed18eEXAMPLE",
    "TagSet": [],
    "VpcId": "vpc-0e12f52b21EXAMPLE"
  }
}

```

Pour attribuer des préfixes IPv6 spécifiques lors de la création de l'interface réseau

Utilisez la [create-network-interface](#) commande et définissez `--ipv6-prefixes` les préfixes. AWS sélectionne les adresses IP dans cette plage. Dans l'exemple suivant, le préfixe CIDR est `2600:1f13:fc2:a700:1768::/80`.

```

$ C:\> aws ec2 create-network-interface \
  --subnet-id subnet-047cfed18eEXAMPLE \
  --description "IPv6 manual example" \
  --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80

```

Exemple de sortie

```

{
  "NetworkInterface": {
    "AvailabilityZone": "us-west-2a",
    "Description": "IPv6 automatic example",
    "Groups": [
      {
        "GroupName": "default",
        "GroupId": "sg-044c2de2c4EXAMPLE"
      }
    ],
    "InterfaceType": "interface",
    "Ipv6Addresses": [],
    "MacAddress": "02:bb:e4:31:fe:09",
    "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
    "OwnerId": "123456789012",
    "PrivateIpAddress": "10.0.0.73",
    "PrivateIpAddresses": [
      {
        "Primary": true,

```

```
        "PrivateIpAddress": "10.0.0.73"
      }
    ],
    "Ipv6Prefixes": [
      {
        "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
      }
    ],
    "RequesterId": "AIDAIV5AJI5LXF5XXDPC0",
    "RequesterManaged": false,
    "SourceDestCheck": true,
    "Status": "pending",
    "SubnetId": "subnet-047cfed18eEXAMPLE",
    "TagSet": [],
    "VpcId": "vpc-0e12f52b21EXAMPLE"
  }
}
```

Attribuer des préfixes aux interfaces réseau existantes

Après avoir attribué les préfixes, utilisez la [attach-network-interface](#) AWS CLI commande pour associer l'interface réseau à votre instance. Vous devez configurer votre système d'exploitation afin de prendre en charge les interfaces réseau avec des préfixes. Pour plus d'informations, consultez [Configurer votre système d'exploitation pour les interfaces réseau avec des préfixes](#).

Tâches

- [Attribuer des préfixes automatiques à une interface réseau existante](#)
- [Attribuer des préfixes spécifiques à une interface réseau existante](#)

Attribuer des préfixes automatiques à une interface réseau existante

Vous pouvez affecter des préfixes automatiques à une interface réseau existante à l'aide de l'une des méthodes suivantes.

Console

Pour attribuer des préfixes automatiques à une interface réseau existante

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).

- Sélectionnez l'interface réseau à laquelle attribuer les préfixes, puis Actions, Manage prefixes (Gérer les préfixes).
- Pour affecter automatiquement un préfixe IPv4, sélectionnez Auto-assign (Affectation automatique) sous IPv4 prefix delegation (Délégation du préfixe IPv4). Ensuite, pour Number of IPv4 prefixes (Nombre de préfixes IPv4), indiquez le nombre de préfixes à affecter.
- Pour affecter automatiquement un préfixe IPv6, sélectionnez Auto-assign (Affectation automatique) sous IPv6 prefix delegation (Délégation du préfixe IPv6). Ensuite, pour Number of IPv6 prefixes (Nombre de préfixes IPv6), indiquez le nombre de préfixes à affecter.

 Note

L'option IPv6 prefix delegation (délégation du préfixe IPv6) s'affiche uniquement si le sous-réseau sélectionné est activé pour IPv6.

- Choisissez Enregistrer.

AWS CLI

Vous pouvez utiliser la commande [assign-ipv6-addresses](#) pour attribuer des préfixes IPv6 et la commande [assign-private-ip-addresses](#) pour attribuer des préfixes IPv4 aux interfaces réseau existantes.

Pour attribuer des préfixes IPv4 automatiques à une interface réseau existante

Utilisez la [assign-private-ip-addresses](#) commande et définissez `--ipv4-prefix-count` le nombre de préfixes que vous souhaitez AWS attribuer. Dans l'exemple suivant, AWS attribue un préfixe 1 IPv4.

```
$ C:\> aws ec2 assign-private-ip-addresses \  
--network-interface-id eni-081fbb4095EXAMPLE \  
--ipv4-prefix-count 1
```

Exemple de sortie

```
{  
  "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",  
  "AssignedIpv4Prefixes": [  
    {  
      "Ipv4Prefix": "10.0.0.176/28"    }  
  ]  
}
```

```
    }  
  ]  
}
```

Pour attribuer des préfixes IPv6 automatiques à une interface réseau existante

Utilisez la commande [assign-ipv6-addresses](#) et définissez le nombre `--ipv6-prefix-count` de préfixes que vous souhaitez attribuer. AWS Dans l'exemple suivant, AWS attribue un préfixe 1 IPv6.

```
$ C:\> aws ec2 assign-ipv6-addresses \  
--network-interface-id eni-00d577338cEXAMPLE \  
--ipv6-prefix-count 1
```

Exemple de sortie

```
{  
  "AssignedIpv6Prefixes": [  
    "2600:1f13:fc2:a700:18bb::/80"  
  ],  
  "NetworkInterfaceId": "eni-00d577338cEXAMPLE"  
}
```

Attribuer des préfixes spécifiques à une interface réseau existante

Vous pouvez affecter des préfixes spécifiques à une interface réseau existante à l'aide de l'une des méthodes suivantes.

Console

Pour affecter des préfixes spécifiques à une interface réseau existante

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez l'interface réseau à laquelle attribuer les préfixes, puis Actions, Manage prefixes (Gérer les préfixes).
4. Pour attribuer un préfixe IPv4 spécifique, sélectionnez Custom (Personnaliser) sous IPv4 prefix delegation (Délégation du préfixe IPv4). Puis sélectionnez Add new prefix (Ajouter un nouveau préfixe) et saisissez le préfixe à utiliser.

5. Pour attribuer un préfixe IPv6 spécifique, sélectionnez Custom (Personnaliser) sous IPv6 prefix delegation (Délégation du préfixe IPv6). Puis sélectionnez Add new prefix (Ajouter un nouveau préfixe) et saisissez le préfixe à utiliser.

 Note

L'option IPv6 prefix delegation (délégation du préfixe IPv6) s'affiche uniquement si le sous-réseau sélectionné est activé pour IPv6.

6. Choisissez Enregistrer.

AWS CLI

Attribuer des préfixes IPv4 spécifiques à une interface réseau existante

Utilisez la [assign-private-ip-addresses](#) commande et définissez `--ipv4-prefixes` le préfixe. AWS sélectionne les adresses IPv4 dans cette plage. Dans l'exemple suivant, le préfixe CIDR est `10.0.0.208/28`.

```
$ C:\> aws ec2 assign-private-ip-addresses \  
--network-interface-id eni-081fbb4095EXAMPLE \  
--ipv4-prefixes 10.0.0.208/28
```

Exemple de sortie

```
{  
  "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",  
  "AssignedIpv4Prefixes": [  
    {  
      "Ipv4Prefix": "10.0.0.208/28"  
    }  
  ]  
}
```

Pour attribuer des préfixes IPv6 automatiques à une interface réseau existante

Utilisez la commande [assign-ipv6-addresses](#) et définissez le préfixe. `--ipv6-prefixes` AWS sélectionne les adresses IPv6 dans cette plage. Dans l'exemple suivant, le préfixe CIDR est `2600:1f13:fc2:a700:18bb::/80`.

```
$ C:\> aws ec2 assign-ipv6-addresses \  
--network-interface-id eni-00d577338cEXAMPLE \  
--ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

Exemple de sortie

```
{  
  "NetworkInterfaceId": "eni-00d577338cEXAMPLE",  
  "AssignedIpv6Prefixes": [  
    {  
      "Ipv6Prefix": "2600:1f13:fc2:a700:18bb::/80"  
    }  
  ]  
}
```

Configurer votre système d'exploitation pour les interfaces réseau avec des préfixes

Les AMI Amazon Linux peuvent contenir des scripts supplémentaires installés par AWS, appelé `ec2-net-utils`. Ces scripts automatisent le cas échéant la configuration de vos interfaces réseau. Ces scripts sont disponibles pour Amazon Linux uniquement.

Si vous n'utilisez pas Amazon Linux, vous pouvez utiliser le plugin Container Network Interface (CNI) pour Kubernetes ou `dockerd` si vous utilisez Docker pour gérer vos conteneurs.

Afficher les préfixes affectés à vos interfaces réseau

Vous pouvez afficher les préfixes affectés à vos interfaces réseau à l'aide de l'une des méthodes suivantes.

Console

Pour afficher les préfixes automatiques affectés à une interface réseau existante

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez l'interface réseau pour laquelle afficher les préfixes et sélectionnez l'onglet Details (Détails).
4. Le champ Délégation du Préfixe IPv4 répertorie les préfixes IPv4 attribués et le champ Délégation de préfixes IPv6 répertorie les préfixes IPv6 attribués.

AWS CLI

Vous pouvez utiliser la [describe-network-interfaces](#) AWS CLI commande pour afficher les préfixes attribués à vos interfaces réseau.

```
$ C:\> aws ec2 describe-network-interfaces
```

Exemple de sortie

```
{
  "NetworkInterfaces": [
    {
      "AvailabilityZone": "us-west-2a",
      "Description": "IPv4 automatic example",
      "Groups": [
        {
          "GroupName": "default",
          "GroupId": "sg-044c2de2c4EXAMPLE"
        }
      ],
      "InterfaceType": "interface",
      "Ipv6Addresses": [],
      "MacAddress": "02:98:65:dd:18:47",
      "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
      "OwnerId": "123456789012",
      "PrivateIpAddress": "10.0.0.62",
      "PrivateIpAddresses": [
        {
          "Primary": true,
          "PrivateIpAddress": "10.0.0.62"
        }
      ],
      "Ipv4Prefixes": [
        {
          "Ipv4Prefix": "10.0.0.208/28"
        }
      ],
      "Ipv6Prefixes": [],
      "RequesterId": "AIDAIV5AJI5LXF5XXDPC0",
      "RequesterManaged": false,
      "SourceDestCheck": true,
      "Status": "available",
      "SubnetId": "subnet-05eef9fb78EXAMPLE",
    }
  ]
}
```

```
    "TagSet": [],
    "VpcId": "vpc-0e12f52b2146bf252"
  },
  {
    "AvailabilityZone": "us-west-2a",
    "Description": "IPv6 automatic example",
    "Groups": [
      {
        "GroupName": "default",
        "GroupId": "sg-044c2de2c411c91b5"
      }
    ],
    "InterfaceType": "interface",
    "Ipv6Addresses": [],
    "MacAddress": "02:bb:e4:31:fe:09",
    "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
    "OwnerId": "123456789012",
    "PrivateIpAddress": "10.0.0.73",
    "PrivateIpAddresses": [
      {
        "Primary": true,
        "PrivateIpAddress": "10.0.0.73"
      }
    ],
    "Ipv4Prefixes": [],
    "Ipv6Prefixes": [
      {
        "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
      }
    ],
    "RequesterId": "AIDAIV5AJI5LXF5XXDPC0",
    "RequesterManaged": false,
    "SourceDestCheck": true,
    "Status": "available",
    "SubnetId": "subnet-05eef9fb78EXAMPLE",
    "TagSet": [],
    "VpcId": "vpc-0e12f52b21EXAMPLE"
  }
]
}
```

Supprimer les préfixes de vos interfaces réseau

Vous pouvez supprimer les préfixes de vos interfaces réseau à l'aide de l'une des méthodes suivantes.

Console

Pour supprimer les préfixes d'une interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez l'interface réseau pour laquelle supprimer des préfixes, puis Actions, Manage prefixes (Gérer les préfixes).
4. Effectuez l'une des actions suivantes :
 - Pour supprimer tous les préfixes affectés, sélectionnez Ne pas affecter, sous Délégation du Préfixe IPv4 et Délégation du Préfixe IPv6.
 - Pour supprimer des préfixes affectés spécifiques, sous Délégation du Préfixe IPv4 ou Délégation du Préfixe IPv6, choisissez Personnaliser, puis Annuler l'affectation en regard des préfixes à supprimer.

Note

L'option IPv6 prefix delegation (délégation du préfixe IPv6) s'affiche uniquement si le sous-réseau sélectionné est activé pour IPv6.

5. Choisissez Enregistrer.

AWS CLI

Vous pouvez utiliser la commande [unassign-ipv6-addresses](#) pour supprimer des préfixes IPv6 et la commande [unassign-private-ip-addresses](#) pour supprimer des préfixes IPv4 aux interfaces réseau existantes.

Pour supprimer les préfixes IPv4 d'une interface réseau

Utilisez la commande [unassign-private-ip-addresses](#) et spécifiez pour `--ipv4-prefix` l'adresse que vous souhaitez supprimer.

```
$ C:\> aws ec2 unassign-private-ip-addresses \  
--network-interface-id eni-081fbb4095EXAMPLE \  
--ipv4-prefixes 10.0.0.176/28
```

Pour supprimer les préfixes IPv6 d'une interface réseau

Utilisez la commande [unassign-ipv6-addresses](#) et spécifiez pour `--ipv6-prefix` l'adresse que vous souhaitez supprimer.

```
$ C:\> aws ec2 unassign-ipv6-addresses \  
--network-interface-id eni-00d577338cEXAMPLE \  
--ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

Bande passante réseau d'instance Amazon EC2

Les spécifications de bande passante de l'instance s'appliquent au trafic entrant et sortant de l'instance. Par exemple, si une instance spécifie jusqu'à 10 Gbit/s de bande passante, cela signifie qu'elle dispose d'une bande passante maximale de 10 Gbit/s pour le trafic entrant et de 10 Gbit/s pour le trafic sortant. La bande passante du réseau dont dispose une instance EC2 dépend de plusieurs facteurs suivants.

Trafic multi-flux

La bande passante pour le trafic multi-flux agrégé disponible pour une instance dépend de la destination du trafic.

- Au sein de la région – Le trafic peut utiliser la bande passante réseau complète disponible pour l'instance.
- Pour les autres régions, une passerelle Internet, Direct Connect ou passerelles locales (LGW) : le trafic peut utiliser jusqu'à 50 % de la bande passante du réseau disponible pour une instance de la génération actuelle avec un minimum de 32 vCPUs. La bande passante pour une instance de génération actuelle avec moins de 32 vCPU est limitée à 5 Gbit/s.

Trafic à flux unique

La bande passante de référence pour le trafic à flux unique est limitée à 5 Gbit/s lorsque les instances ne sont pas dans le même [groupe de placement du cluster](#). Pour réduire la latence et augmenter la bande passante à flux unique, essayez l'une des solutions suivantes :

- Utilisez un groupe de placement du cluster pour obtenir jusqu'à 10 Gbit/s de bande passante pour les instances au sein du même groupe.
- Configurez plusieurs chemins entre deux points de terminaison pour obtenir une bande passante plus élevée avec Multipath TCP (MPTCP).
- Configurez ENA Express pour les instances éligibles au sein du même sous-réseau afin d'atteindre 25 Gbit/s entre ces instances.

Bande passante d'instance disponible

La bande passante réseau disponible d'une instance dépend du nombre de vCPU dont elle dispose. Par exemple, une instance `m5.8xlarge` dispose de 32 vCPU et d'une bande passante réseau de 10 Gbit/s, et une instance `m5.16xlarge` dispose de 64 vCPU et de 20 Gbit/s de bande passante réseau. Les instances peuvent ne pas atteindre cette bande passante, par exemple, si elles dépassent les autorisations réseau au niveau de l'instance, tels que le paquet par seconde ou le nombre de connexions suivies. La quantité de bande passante disponible exploitable par le trafic dépend du nombre de vCPUs et de la destination. Par exemple, si une instance `m5.16xlarge` dispose de 64 vCPU, alors le trafic vers une autre instance de la Région pourra utiliser la bande passante totale disponible (20 Gbit/s). Toutefois, le trafic vers une autre instance dans une Région différente ne peut utiliser que 50 % de la bande passante disponible (10 Gbit/s).

Généralement, pour les instances avec 16 vCPU ou moins (taille `4xlarge` et plus petites) les références indiquent une bande passante « maximum » spécifiée ; par exemple, « jusqu'à 10 Gbit/s ». Ces instances ont une bande passante de base. Pour répondre à une demande supplémentaire, ils peuvent utiliser un mécanisme de crédit d'I/O réseau pour surpasser leur bande passante de base. Les instances peuvent utiliser la bande passante de rafale pendant une durée limitée, généralement de 5 à 60 minutes, en fonction de la taille de l'instance.

Une instance reçoit le nombre maximal de crédits d'I/O réseau au lancement. Si l'instance épuise ses crédits d'I/O réseau, elle retourne à sa bande passante de base. Une instance en cours d'exécution gagne des crédits d'I/O réseau lorsqu'elle utilise moins de bande passante réseau que sa bande passante de base. Une instance arrêtée ne gagne pas de crédits d'I/O réseau. Le mode rafale d'une instance dépend de la mesure du possible, même lorsque l'instance dispose de crédits disponibles, car la bande passante de rafale est une ressource partagée.

Il existe des compartiments de crédits d'E/S réseau distincts pour les trafics entrants et sortants.

Performances réseau de base et de rafale

Le guide des types d'instances Amazon EC2 décrit les performances réseau pour chaque type d'instance, ainsi que la bande passante réseau de référence disponible pour les instances qui peuvent utiliser de la bande passante en rafale. Pour plus d'informations, consultez les ressources suivantes :

- [Spécifications du réseau — Usage général](#)
- [Spécifications du réseau — Optimisé pour le calcul](#)
- [Spécifications du réseau — Mémoire optimisée](#)
- [Spécifications du réseau — Stockage optimisé](#)
- [Spécifications du réseau — Calcul accéléré](#)
- [Spécifications du réseau — Calcul à haute performance](#)
- [Spécifications du réseau — Génération précédente](#)

Pour visualiser les performances du réseau à l'aide du AWS CLI

Vous pouvez utiliser la AWS CLI commande [describe-instance-types](#) pour afficher des informations sur un type d'instance. L'exemple suivant affiche les informations de performances du réseau pour toutes les instances C5.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*"
--query "InstanceTypes[][InstanceType, NetworkInfo.NetworkPerformance,
NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps]" --output table
```

```
-----
|           DescribeInstanceTypes           |
+-----+-----+-----+
| c5.4xlarge | Up to 10 Gigabit | 5.0 |
| c5.xlarge  | Up to 10 Gigabit | 1.25 |
| c5.12xlarge | 12 Gigabit       | 12.0 |
| c5.24xlarge | 25 Gigabit       | 25.0 |
| c5.metal   | 25 Gigabit       | 25.0 |
| c5.9xlarge | 12 Gigabit       | 12.0 |
| c5.2xlarge | Up to 10 Gigabit | 2.5 |
| c5.large   | Up to 10 Gigabit | 0.75 |
| c5.18xlarge | 25 Gigabit       | 25.0 |
+-----+-----+-----+
```

Contrôle de la bande passante de l'instance

Vous pouvez utiliser CloudWatch des métriques pour surveiller la bande passante du réseau de l'instance ainsi que les paquets envoyés et reçus. Vous pouvez utiliser les métriques de performances réseau fournies par le pilote Elastic Network Adapter (ENA) pour contrôler lorsque le trafic dépasse les autorisations réseau définies par Amazon EC2 au niveau de l'instance.

Vous pouvez configurer si Amazon EC2 envoie des données métriques pour l'instance en CloudWatch utilisant des périodes d'une minute ou de cinq minutes. Il est possible que les métriques de performance du réseau indiquent qu'une allocation a été dépassée et que des paquets ont été abandonnés alors que les métriques d' CloudWatch instance ne le font pas. Cela peut se produire lorsque l'instance connaît un bref pic de demande de ressources réseau (connu sous le nom de microrafale), mais que les CloudWatch métriques ne sont pas suffisamment détaillées pour refléter ces pics de microsecondes.

En savoir plus

- [Métriques des instances](#)
- [Métriques des performances réseau](#)

Mise en réseau améliorée sur Amazon EC2

La mise en réseau améliorée utilise la virtualisation d'I/O d'une racine unique (SR-IOV) pour fournir des fonctionnalités de mise en réseau hautes performances sur les [types d'instance pris en charge](#). La méthode SR-IOV de virtualisation des appareils fournit de meilleures performances des I/O et une utilisation de la CPU réduite par rapport aux interfaces réseau virtualisées traditionnelles. La mise en réseau améliorée offre une bande passante supérieure, des performances de paquet par seconde (PPS) nettement plus élevées, ainsi que des latences réduites entre les instances. L'utilisation de la mise en réseau améliorée n'implique aucun coût supplémentaire.

Pour plus d'informations sur la vitesse réseau prise en charge pour chaque type d'instance, consultez [Types d'instances Amazon EC2](#).

Sommaire

- [Prise en charge de la mise en réseau améliorée](#)
- [Activez une mise en réseau améliorée avec l'Elastic Network Adapter \(ENA\) sur vos instances EC2](#)
- [Améliorez les performances du réseau avec ENA Express sur vos instances EC2](#)

- [Activez une mise en réseau améliorée avec l'interface Intel 82599 VF sur vos instances EC2](#)
- [Contrôlez les performances réseau de votre instance EC2](#)
- [Résoudre les problèmes liés à l'adaptateur réseau Elastic sous Linux](#)
- [Résoudre les problèmes liés au pilote Windows d'Elastic Network Adapter](#)
- [Amélioration de la latence réseau pour les instances Amazon EC2 basées sur Linux](#)
- [Considérations relatives au système Nitro pour le réglage des performances](#)
- [Optimisation des performances réseau sur les instances Windows](#)

Prise en charge de la mise en réseau améliorée

Tous les types d'instance de génération actuelle prennent en charge la mise en réseau améliorée, à l'exception des instances T2.

Vous pouvez activer la mise en réseau améliorée à l'aide de l'un des mécanismes suivants :

Elastic Network Adapter (ENA)

L'Adaptateur réseau élastique (ENA) prend en charge des vitesses réseau allant jusqu'à 100 Gbit/s pour les types d'instances pris en charge.

Toutes les [instances basées sur le système AWS Nitro](#) utilisent l'ENA pour améliorer la mise en réseau. En outre, les types d'instances Xen suivants prennent en charge l'ENA : H1, G3, m4.16xlarge, P2, P3, P3dn et R4.

Pour plus d'informations, consultez [Activez une mise en réseau améliorée avec l'Elastic Network Adapter \(ENA\) sur vos instances EC2](#).

Interface Intel 82599 Virtual Function (VF)

L'interface Intel 82599 Virtual Function prend en charge les vitesses réseau allant jusqu'à 10 Gbit/s pour les types d'instance pris en charge.

Les types d'instance suivants utilisent l'interface Intel 82599 VF pour la mise en réseau améliorée : C3, C4, D2, I2, M4 (sauf m4.16xlarge) et R3.

Pour plus d'informations, consultez [Activez une mise en réseau améliorée avec l'interface Intel 82599 VF sur vos instances EC2](#).

Activez une mise en réseau améliorée avec l'Elastic Network Adapter (ENA) sur vos instances EC2

Amazon EC2 offre des fonctionnalités de mise en réseau améliorée via l'adaptateur Elastic Network Adapter (ENA). Pour utiliser la mise en réseau améliorée, vous devez installer le module ENA requis et activer la prise en charge ENA.

Table des matières

- [Prérequis](#)
- [Performances réseau améliorées](#)
- [AMI Linux avec le module requis](#)
- [Tester l'activation de réseaux améliorés](#)
- [Activer les réseaux améliorés sur une instance](#)
- [Notes de mise à jour du pilote](#)

Prérequis

Pour préparer la mise en réseau améliorée à l'aide de l'adaptateur réseau ENA, configurez votre instance comme suit :

- Lancez une [instance basée sur le système AWS Nitro](#).
- Vérifiez que l'instance a une connectivité Internet.
- Si l'instance comporte des données importantes que vous souhaitez conserver, vous devez les sauvegarder maintenant en créant une AMI à partir de votre instance. La mise à jour des noyaux et des modules noyau, ainsi que l'activation de l'attribut `enaSupport`, peuvent rendre les instances incompatibles ou les systèmes d'exploitation inaccessibles. Si cela se produit et que vous disposez d'une sauvegarde récente, vos données continueront d'être conservées.
- Instances Linux : lancez l'instance à l'aide d'une version prise en charge du noyau Linux et d'une distribution prise en charge, afin que la mise en réseau améliorée ENA soit automatiquement activée pour votre instance. Pour plus d'informations, consultez [ENA Linux Kernel Driver Release Notes](#).
- Instances Windows : si l'instance exécute Windows Server 2008 R2 SP1, assurez-vous qu'elle dispose de la mise à jour du support de [signature de code SHA-2](#).
- [AWS CloudShell](#) Utilisez-le depuis ou installez et configurez le [AWS CLI](#) ou [AWS Tools for Windows PowerShell](#) sur n'importe quel ordinateur de votre choix, de préférence sur votre ordinateur de

bureau ou portable local. AWS Management Console Pour plus d'informations, consultez la section [Accès à Amazon EC2](#) du [Guide de l'utilisateur AWS CloudShell](#). La gestion de la mise en réseau améliorée n'est pas possible à partir de la console Amazon EC2.

Performances réseau améliorées

La documentation suivante fournit un résumé des performances réseau pour les types d'instance qui prennent en charge la mise en réseau améliorée ENA :

- [Spécifications réseau pour les instances de calcul accéléré](#)
- [Spécifications réseau pour les instances optimisées pour le calcul](#)
- [Spécifications réseau pour les instances à usage général](#)
- [Spécifications réseau pour les instances de calcul hautes performances](#)
- [Spécifications réseau pour les instances optimisées en mémoire](#)
- [Spécifications réseau pour les instances optimisées pour le stockage](#)

AMI Linux avec le module requis

Les AMI suivantes incluent le module ENA requis et la prise en charge ENA est activée :

- AL2023
- Amazon Linux 2
- Amazon Linux AMI 2018.03 et version ultérieure
- Ubuntu 14.04 ou une version ultérieure avec noyau `linux-aws`

Note

AWS Les types d'instances basés sur Graviton nécessitent Ubuntu 18.04 ou version ultérieure avec noyau `linux-aws`

- Red Hat Enterprise Linux 7.4 ou une version ultérieure
- SUSE Linux Enterprise Server 12 SP2 ou une version ultérieure
- CentOS 7.4.1708 ou une version ultérieure
- FreeBSD 11.1 ou une version ultérieure

- Debian GNU/Linux 9 ou version ultérieure

Pour vérifier si la mise en réseau améliorée est déjà activée, vérifiez que le ena module est installé sur votre instance et que l'enaSupport attribut est défini. Si tel est le cas, la commande `ethtool -i ethn` doit indiquer que le module est utilisé sur l'interface réseau.

Module noyau (ena)

Pour vérifier que le module ena est installé, utilisez la commande `modinfo` comme illustré dans l'exemple suivant :

```
[ec2-user ~]$ modinfo ena
filename:    /lib/modules/4.14.33-59.37.amzn2.x86_64/kernel/drivers/amazon/net/ena/
ena.ko
version:    1.5.0g
license:    GPL
description: Elastic Network Adapter (ENA)
author:     Amazon.com, Inc. or its affiliates
srcversion: 692C7C68B8A9001CB3F31D0
alias:      pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:      pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:      pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:      pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
retpoline:  Y
intree:    Y
name:      ena
...
```

Dans l'instance Amazon Linux, le ena module est installé.

```
ubuntu:~$ modinfo ena
ERROR: modinfo: could not find module ena
```

Dans l'instance Ubuntu, le module n'est pas installé, vous devez donc d'abord l'installer. Pour plus d'informations, consultez [Ubuntu](#).

Tester l'activation de réseaux améliorés

Vous pouvez tester si la mise en réseau améliorée est activée dans vos instances ou dans vos AMI.

Attribut d'instance

Pour vérifier si l'attribut de mise en réseau améliorée `enaSupport` est défini sur une instance, utilisez l'une des commandes suivantes. Si l'attribut est défini, la réponse est `true`.

- [describe-instances](#) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query  
"Reservations[].Instances[].EnaSupport"
```

- [Get-EC2Instance](#) (Outils pour Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

Attribut d'image

Pour vérifier si l'attribut de mise en réseau améliorée `enaSupport` est déjà défini sur une AMI, utilisez l'une des commandes suivantes. Si l'attribut est défini, la réponse est `true`.

- [describe-images](#) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[].EnaSupport"
```

- [Get-EC2Image](#) (Outils pour Windows PowerShell)

```
(Get-EC2Image -ImageId ami_id).EnaSupport
```

pilote d'interface réseau Linux

Utilisez la commande suivante pour vérifier que le module `ena` est utilisé sur une interface particulière, en remplaçant le nom de l'interface par celui que vous voulez contrôler. Si vous utilisez une seule interface (par défaut), ce sera `eth0`. Si le système d'exploitation prend en charge les [noms de réseau prévisibles](#), il peut s'agir d'un nom tel que `ens5`.

Dans l'exemple suivant, le module `ena` n'est pas chargé, car le pilote affiché est `vif`.

```
[ec2-user ~]$ ethtool -i eth0  
driver: vif  
version:
```

```
firmware-version:  
bus-info: vif-0  
supports-statistics: yes  
supports-test: no  
supports-EEPROM-access: no  
supports-register-dump: no  
supports-priv-flags: no
```

Dans cet exemple, le module ena est chargé avec la version minimale recommandée. La mise en réseau améliorée est correctement configurée pour cette instance.

```
[ec2-user ~]$ ethtool -i eth0  
driver: ena  
version: 1.5.0g  
firmware-version:  
expansion-rom-version:  
bus-info: 0000:00:05.0  
supports-statistics: yes  
supports-test: no  
supports-EEPROM-access: no  
supports-register-dump: no  
supports-priv-flags: no
```

Activer les réseaux améliorés sur une instance

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Amazon Linux

Amazon Linux 2 et les dernières versions de Amazon Linux AMI incluent le module requis pour la mise en réseau améliorée avec ENA installé et la prise en charge ENA activée. Par conséquent, si vous lancez une instance avec la dernière version HVM d'Amazon Linux sur un type d'instance pris en charge, la mise en réseau améliorée est déjà activée pour votre instance. Pour plus d'informations, consultez [Tester l'activation de réseaux améliorés](#).

Si vous avez lancé votre instance avec une version d'Amazon Linux AMI plus ancienne et que la mise en réseau améliorée n'est pas activée sur cette dernière, utilisez le procédure suivante pour l'activer.

Pour activer la mise en réseau améliorée sur Amazon Linux AMI

1. Connectez-vous à votre instance.

2. Depuis l'instance, exécutez la commande suivante pour mettre à jour votre instance avec le noyau et les modules noyau les plus récents, y compris ena :

```
[ec2-user ~]$ sudo yum update
```

3. Depuis votre ordinateur local, réinitialisez votre instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [reboot-instances](#) (AWS CLI), [Restart-EC2Instance](#) (AWS Tools for Windows PowerShell).
4. Connectez-vous à nouveau à votre instance et vérifiez que le module ena est installé et possède la version minimale recommandée à l'aide de la commande `modinfo ena` depuis [Tester l'activation de réseaux améliorés](#).
5. [Instance basée sur EBS] À partir de votre ordinateur local, arrêtez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [stop-instances](#) (AWS CLI), [Stop-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

[Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Vous devez utiliser cette procédure : [Pour activer la mise en réseau améliorée sur Amazon Linux AMI \(instances basées sur le stockage d'instance\)](#).

6. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:
 - [modify-instance-attribute](#) (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance-id --ena-support
```

- [Edit-EC2InstanceAttribute](#) (Outils pour Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
```

7. (Facultatif) Créez une AMI à partir de l'instance, comme décrit dans [Création d'une AMI basée sur Amazon EBS](#). L'AMI hérite de l'attribut `enaSupport` de mise en réseau améliorée de l'instance. Par conséquent, vous pouvez utiliser cet AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.
8. Depuis votre ordinateur local, démarrez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [start-instances](#) (AWS CLI), [Start-EC2Instance](#) (AWS Tools for

Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.

9. Connectez-vous à votre instance et vérifiez que le module `ena` est installé et chargé sur votre interface réseau à l'aide de la commande `ethtool -i ethn` depuis [Tester l'activation de réseaux améliorés](#).

Si vous ne parvenez pas à vous connecter à votre instance après avoir activé la mise en réseau améliorée, consultez [Résoudre les problèmes liés à l'adaptateur réseau Elastic sous Linux](#).

Pour activer la mise en réseau améliorée sur Amazon Linux AMI (instances basées sur le stockage d'instance)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez une nouvelle AMI comme décrit dans [Créer une AMI Linux basée sur le stockage d'instance](#), en veillant à activer l'attribut de mise en réseau améliorée lors de l'enregistrement de l'AMI.

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

Ubuntu

Les dernières AMI HVM Ubuntu incluent le module requis pour la mise en réseau améliorée avec ENA installé et la prise en charge ENA activée. Par conséquent, si vous lancez une instance avec la dernière AMI HVM Ubuntu sur un type d'instance pris en charge, la mise en réseau améliorée est déjà activée pour votre instance. Pour plus d'informations, consultez [Tester l'activation de réseaux améliorés](#).

Si vous avez lancé votre instance à l'aide d'une AMI plus ancienne et que la mise en réseau améliorée n'est pas déjà activée pour celle-ci, vous pouvez installer le package noyau `linux-aws` pour obtenir les pilotes de mise en réseau améliorée les plus récents et mettre à jour l'attribut requis.

Pour installer le package du noyau **linux-aws** (Ubuntu 16.04 ou version ultérieure)

Ubuntu 16.04 et 18.04 sont fournis avec le noyau personnalisé Ubuntu (package du noyau `linux-aws`). Pour utiliser un autre noyau, contactez [AWS Support](#).

Pour installer le package du noyau **linux-aws** (Ubuntu Trusty 14.04)

1. Connectez-vous à votre instance.
2. Mettez à jour le cache du package et les packages.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

Important

Si, lors d'une mise à jour, vous êtes invité à installer grub, utilisez `/dev/xvda` pour y installer grub, puis choisissez de conserver la version courante de `/boot/grub/menu.lst`.

3. [Instance basée sur EBS] À partir de votre ordinateur local, arrêtez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [stop-instances](#) (AWS CLI), [Stop-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

[Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Vous devez utiliser cette procédure : [Pour activer la mise en réseau améliorée sur Ubuntu \(instances basées sur le stockage d'instance\)](#).

4. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:

- [modify-instance-attribute](#) (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute](#) (Outils pour Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
```

5. (Facultatif) Créez une AMI à partir de l'instance, comme décrit dans [Création d'une AMI basée sur Amazon EBS](#). L'AMI hérite de l'attribut `enaSupport` de mise en réseau améliorée de

l'instance. Par conséquent, vous pouvez utiliser cet AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.

6. Depuis votre ordinateur local, démarrez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [start-instances](#) (AWS CLI), [Start-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.

Pour activer la mise en réseau améliorée sur Ubuntu (instances basées sur le stockage d'instance)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez une nouvelle AMI comme décrit dans [Créer une AMI Linux basée sur le stockage d'instance](#), en veillant à activer l'attribut de mise en réseau améliorée lors de l'enregistrement de l'AMI.

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

RHEL, SUSE, CentOS

Les dernières AMI pour Red Hat Enterprise Linux, SUSE Linux Enterprise Server et CentOS incluent le module requis pour une mise en réseau améliorée avec ENA et ont la prise en charge ENA activée. Par conséquent, si vous lancez une instance avec la dernière AMI HVM Ubuntu sur un type d'instance pris en charge, la mise en réseau améliorée est déjà activée pour votre instance. Pour plus d'informations, consultez [Tester l'activation de réseaux améliorés](#).

La procédure suivante fournit les étapes générales pour activer la mise en réseau améliorée via ENA sur une distribution Linux autre qu'Amazon Linux AMI ou Ubuntu. Pour plus d'informations, telles que la syntaxe détaillée des commandes, les emplacements de fichier ou la prise en charge des packages et des outils, consultez la documentation spécifique de votre distribution Linux.

Pour activer la mise en réseau améliorée sur Linux

1. Connectez-vous à votre instance.

2. Clonez le code source du ena module sur votre instance GitHub à partir de <https://github.com/amzn/amzn-drivers>. (SUSE Linux Enterprise Server 12 SP2 et versions ultérieures incluent ENA 2.02 par défaut, de sorte que vous n'êtes pas tenu de télécharger ni de compiler le pilote ENA. Pour SUSE Linux Enterprise Server 12 SP2 et versions ultérieures, vous devez déposer une demande d'ajout de la version du pilote que vous souhaitez dans le noyau de base).

```
git clone https://github.com/amzn/amzn-drivers
```

3. Compilez et installez le module ena sur votre instance. Ces étapes dépendent de la distribution Linux. Pour plus d'informations sur la compilation du module sur Red Hat Enterprise Linux, consultez [Comment installer le dernier pilote ENS pour une meilleure prise en charge réseau sur une instance Amazon EC2 qui exécute RHEL ?](#)
4. Exécutez la commande `sudo depmod` pour mettre à jour les dépendances du module.
5. Mettez à jour `initramfs` sur votre instance pour garantir que le nouveau module se charge au démarrage. Par exemple, si votre distribution prend en charge `dracut`, vous pouvez utiliser la commande suivante :

```
dracut -f -v
```

6. Déterminez si par défaut votre système utilise des noms d'interface réseau prévisibles. Les systèmes qui utilisent `systemd` ou `udev` version 197 ou supérieure peuvent renommer les périphériques Ethernet et ne garantissent pas qu'une seule interface réseau sera nommée `eth0`. Ce comportement peut entraîner des problèmes de connexion à votre instance. Pour plus d'informations et pour voir les autres options de configuration, consultez la section sur les [noms d'interface réseau prévisibles](#) sur le site web de freedesktop.org.
 - a. Vous pouvez vérifier les versions `systemd` ou `udev` sur les systèmes RPM en utilisant la commande suivante :

```
rpm -qa | grep -e '^systemd-[0-9]\+\|udev-[0-9]\+'  
systemd-208-11.el7_0.2.x86_64
```

Dans l'exemple Red Hat Enterprise Linux 7 ci-dessus, la version `systemd` est 208, de sorte que les noms d'interface réseau prévisibles doivent être désactivés.

- b. Désactivez les noms d'interface réseau prévisibles en ajoutant l'option `net.ifnames=0` à la ligne `GRUB_CMDLINE_LINUX` dans `/etc/default/grub`.

```
sudo sed -i '/^GRUB_CMDLINE_LINUX/s/\ "$/\ net\.ifnames=0\ "' /etc/default/grub
```

- c. Générez à nouveau le fichier de configuration grub.

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Instance basée sur EBS] À partir de votre ordinateur local, arrêtez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [stop-instances](#) (AWS CLI), [Stop-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

[Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Vous devez utiliser cette procédure : [Pour activer les réseaux améliorés sur Linux \(instances basées sur le stockage d'instances\)](#).

8. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée enaSupport à l'aide de l'une des commandes suivantes:

- [modify-instance-attribute](#) (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute](#) (Outils pour Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
```

9. (Facultatif) Créez une AMI à partir de l'instance, comme décrit dans [Création d'une AMI basée sur Amazon EBS](#). L'AMI hérite de l'attribut enaSupport de mise en réseau améliorée de l'instance. Par conséquent, vous pouvez utiliser cet AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.

Si le système d'exploitation de votre instance contient un fichier `/etc/udev/rules.d/70-persistent-net.rules`, vous devez le supprimer avant de créer l'AMI. Ce fichier contient l'adresse MAC de la carte Ethernet de l'instance d'origine. Si une autre instance démarre avec ce fichier, le système d'exploitation ne pourra pas trouver le périphérique et il se peut que `eth0` échoue, entraînant des problèmes de démarrage. Le fichier est à nouveau généré au cycle de démarrage suivant et les instances lancées depuis l'AMI créent leur propre version du fichier.

10. Depuis votre ordinateur local, démarrez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [start-instances](#) (AWS CLI), [Start-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.
11. (Facultatif) Connectez-vous à votre instance et vérifiez que le module est installé.

Si vous ne parvenez pas à vous connecter à votre instance après avoir activé la mise en réseau améliorée, consultez [Résoudre les problèmes liés à l'adaptateur réseau Elastic sous Linux](#).

Pour activer les réseaux améliorés sur Linux (instances basées sur le stockage d'instances)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez une nouvelle AMI comme décrit dans [Créer une AMI Linux basée sur le stockage d'instance](#), en veillant à activer l'attribut de mise en réseau améliorée lors de l'enregistrement de l'AMI.

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu avec DKMS

Cette méthode est fournie à des fins de test et de rétroaction uniquement. Elle n'est pas destinée à être utilisée avec des déploiements en production. Pour plus d'informations sur les déploiements en production, consultez [Ubuntu](#).

Important

L'utilisation de DKMS annule le contrat de support pour votre abonnement. Il ne doit pas être utilisé pour les déploiements de production.

Pour activer la mise en réseau améliorée via ENA sur Ubuntu (instances basées sur EBS)

1. Suivez les étapes 1 et 2 dans [Ubuntu](#).

2. Installez les packages `build-essential` pour compiler le module noyau et les packages `dkms` pour que le module `ena` soit recréé chaque fois que votre noyau est mis à jour.

```
ubuntu:~$ sudo apt-get install -y build-essential dkms
```

3. Clonez la source du `ena` module sur votre instance GitHub à partir de <https://github.com/amzn/amzn-drivers>.

```
ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
```

4. Déplacez le package `amzn-drivers` vers le répertoire `/usr/src/` afin que DKMS puisse le trouver et le générer à chaque mise à jour du noyau. Ajoutez le numéro de version (que vous trouverez dans les notes de version) du code source au nom du répertoire. Par exemple, la version `1.0.0` apparaît dans l'exemple suivant.

```
ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
```

5. Créez le fichier de configuration DKMS avec les valeurs suivantes, en remplaçant votre version d'`ena`.

Créez le fichier.

```
ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
```

Modifiez le fichier et ajoutez les valeurs suivantes.

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Ajoutez, générez et installez le module `ena` sur votre instance à l'aide de DKMS.

Ajoutez le module à DKMS.

```
ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
```

Générez le module avec la commande dkms.

```
ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
```

Installez le module avec dkms.

```
ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
```

7. Générez à nouveau initramfs afin que le module approprié soit chargé au démarrage.

```
ubuntu:~$ sudo update-initramfs -u -k all
```

8. Vérifiez que le module ena est installé à l'aide de la commande modinfo ena depuis [Tester l'activation de réseaux améliorés](#).

```
ubuntu:~$ modinfo ena
filename:    /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
version:    1.0.0
license:    GPL
description: Elastic Network Adapter (ENA)
author:     Amazon.com, Inc. or its affiliates
srcversion: 9693C876C54CA64AE48F0CA
alias:      pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:      pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:      pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:      pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:   3.13.0-74-generic SMP mod_unload modversions
parm:      debug:Debug level (0=none,...,16=all) (int)
parm:      push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
            0 - Automatically choose according to device capability (default)
            1 - Don't push anything to device memory
            3 - Push descriptors and header buffer to device memory (int)
parm:      enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:      enable_missing_tx_detection:Enable missing Tx completions. (default=1)
            (int)
parm:      numa_node_override_array:Numa node override map
            (array of int)
```

```
parm:      numa_node_override:Enable/Disable numa node override (0=disable)
(int)
```

9. Passez à l'étape 3 dans [Ubuntu](#).

Activer les réseaux améliorés sur Windows

Si vous avez lancé votre instance et qu'elle n'a pas la mise en réseau déjà activée, vous devez télécharger et installer le pilote de la carte réseau requis sur votre instance, puis définir l'attribut d'instance `enaSupport` pour activer la mise en réseau améliorée. Vous pouvez uniquement activer cet attribut sur les types d'instance pris en charge et seulement si le pilote ENA est installé. Pour plus d'informations, consultez [Prise en charge de la mise en réseau améliorée](#).

Pour activer la mise en réseau améliorée

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. [Windows Server 2016 et 2019 uniquement] Exécutez le PowerShell script EC2Launch suivant pour configurer l'instance une fois le pilote installé.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

3. Depuis l'instance, installez le pilote comme suit :
 - a. [Téléchargez](#) le pilote le plus récent sur l'instance.
 - b. Décompressez l'archive zip.
 - c. Installez le pilote en exécutant le `install.ps1` PowerShell script.

Note

Si vous obtenez une erreur d'exécution de la stratégie, définissez la stratégie sur `Unrestricted` (par défaut, elle est définie sur `Restricted` ou `RemoteSigned`). Dans une ligne de commande, exécutez `Set-ExecutionPolicy - ExecutionPolicy Unrestricted`, puis réexécutez le `install.ps1` PowerShell script.

4. Depuis votre ordinateur local, arrêtez votre instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [stop-instances](#) (AWS CLI/AWS CloudShell), [Stop-EC2Instance](#)

(AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

5. Activez la prise en charge ENA sur votre instance comme suit :

a. Sur votre ordinateur local, vérifiez l'attribut de prise en charge ENA de l'instance EC2 sur votre instance en exécutant l'une des commandes suivantes. Si l'attribut n'est pas activé, la sortie indiquera « [] » ou une valeur vide. `EnaSupport` est défini sur `false` par défaut.

- [describe-instances](#) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query  
"Reservations[].Instances[].EnaSupport"
```

- [Get-EC2Instance](#) (Outils pour Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

b. Pour activer la prise en charge ENA, exécutez l'une des commandes suivantes :

- [modify-instance-attribute](#) (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

Si vous rencontrez des problèmes lorsque vous redémarrez l'instance, vous pouvez également désactiver la prise en charge ENA à l'aide d'une des commandes suivantes :

- [modify-instance-attribute](#) (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
```

- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $false
```

- c. Vérifiez que l'attribut a été défini sur `true` à l'aide de `describe-instances` ou `Get-EC2Instance` comme indiqué précédemment. Vous devriez désormais voir la sortie suivante :

```
[
  true
]
```

6. Depuis votre ordinateur local, démarrez votre instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [start-instances](#) (AWS CLI/AWS CloudShell), [Start-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance à l'aide de la AWS OpsWorks console afin que son état reste synchronisé.
7. Sur l'instance, vérifiez que le pilote ENA est installé et activé comme suit :
 - a. Cliquez sur l'icône réseau avec le bouton droit de la souris et choisissez Open Network and Sharing Center (Ouvrir le Centre Réseau et partage).
 - b. Choisissez la carte Ethernet (par exemple, Ethernet 2).
 - c. Sélectionnez Details (Détails). Pour Network Connection Details (Détails de connexion réseau), vérifiez que Description a pour valeur Amazon Elastic Network Adapter.
8. Créez une AMI à partir de l'instance (facultatif). L'AMI hérite de l'attribut `enaSupport` à partir de l'instance. Par conséquent, vous pouvez utiliser cette AMI pour lancer une autre instance avec ENA activée par défaut.

Notes de mise à jour du pilote

pilote ENA pour Linux

Pour en savoir plus sur les versions du pilote Linux ENA, consultez les [notes de mise à jour du pilote de noyau Linux ENA](#).

pilote Windows ENA

Les AMI Windows comprennent le pilote Amazon ENA pour activer la mise en réseau améliorée

Le tableau suivant indique la version du pilote ENA à télécharger pour chaque version de Windows Server.

Version Windows Server	Version de pilote ENA
Windows Server 2022	2.4.0 et versions ultérieures
Windows Server 2019	dernières
Windows Server 2016	dernières
Windows Server 2012 R2	2.6.0 et versions antérieures
Windows Server 2012	2.6.0 et versions antérieures
Windows Server 2008 R2	2.2.3 et version antérieure

Le tableau suivant résume les modifications pour chaque version.

Versions du pilote	Détails	Date de publication
2.7.0	<p>Nouvelles fonctions</p> <ul style="list-style-type: none"> • Suppression du support pour Windows Server 2012 (Windows 8) et Windows Server 2012 R2 (Windows 8.1). Le support de ces versions du système d'exploitation a expiré depuis AWS. L'installation du pilote échouera sous Windows Server 2012 et versions antérieures. • Ajout de la prise en charge du transfert du calcul de la somme de contrôle IPv6 Tx vers l'appareil. • Ajout d'une large prise en charge de la file d'attente à faible latence (LLQ). Ceci est activé dynamiquement en fonction des recommandations de l'appareil. Vous 	1er mai 2024

Versions du pilote	Détails	Date de publication
	<p>pouvez remplacer ce paramètre par la nouvelle clé de registre « WidellQ ».</p> <ul style="list-style-type: none">• Ajout de rapports pour les pertes de paquets résultant d'un dépassement de Rx, ce qui indique un espace insuffisant dans l'anneau Rx pour les paquets entrants.• Ajout de la prise en charge des notifications de configuration sous-optimales provenant de l'appareil. Consultez l'ID de l'événement 59000 dans l'observateur d'événements Windows. <p>Correctifs de bogue</p> <ul style="list-style-type: none">• Évitez toute réinitialisation inutile du périphérique provoquée par des paquets Tx dont les en-têtes dépassent la taille d'en-tête LLQ (Low Latency Queuing) maximale.	

Versions du pilote	Détails	Date de publication
2.6.0	<p>Nouvelles fonctions</p> <ul style="list-style-type: none">• Ajoute les métriques de performances réseau suivantes pour les types d'instance qui prennent en charge ENA Express.<ul style="list-style-type: none">• <code>ena_srd_mode</code>• <code>ena_srd_tx_pkts</code>• <code>ena_srd_eligible_tx_pkts</code>• <code>ena_srd_rx_pkts</code>• <code>ena_srd_resource_utilization</code>• Ajoute la métrique de performance réseau <code>conntrack_allowance_available</code> pour les types d'instance basés sur Nitro.• Ajoute un nouveau motif de réinitialisation de l'adaptateur en raison de la détection d'une corruption des données RX.• Met à jour l'infrastructure de journalisation des pilotes. <p>Correctifs de bogue</p> <ul style="list-style-type: none">• Empêche la réinitialisation de l'adaptateur dans le cas où une pénurie de CPU entraîne l'échec de la mise à jour des métriques de performance du réseau.•	20 juin 2023

Versions du pilote	Détails	Date de publication
	<p>Empêche la fausse détection d'une interruption de la pulsation de l'appareil.</p> <ul style="list-style-type: none">• Corrige le script d'installation du pilote pour prendre en charge l'opération de rétrogradation.• Corrige les statistiques relatives au nombre d'erreurs de réception.	
2.5.0	<p>Annonce</p> <p>Le pilote Windows ENA version 2.5.0 a été annulé en raison d'un échec d'initialisation sur le contrôleur de domaine Windows. Windows Client et Windows Server ne sont pas affectés.</p>	17 février 2023

Versions du pilote	Détails	Date de publication
2.4.0	<p>Nouvelles fonctions</p> <ul style="list-style-type: none">• Ajout de la prise en charge de Windows Server 2022.• Supprime la prise en charge de Windows Server 2008 R2.• Définit la file d'attente à faible latence (LLQ) sur Always on (Toujours active) pour améliorer les performances des instances Amazon EC2 de 6e génération. <p>Correctif de bogue.</p> <ul style="list-style-type: none">• Corrige un échec de publication des métriques de performances réseau sur le système de compteur de performances pour Windows (PCW).• Corrige une fuite de mémoire lors de l'opération de lecture des clés de registre.• Empêche une boucle de réinitialisation infinie en cas d'erreur irrécupérable lors du processus de réinitialisation de dispositif.	28 avril 2022

Versions du pilote	Détails	Date de publication
2.2.4	<p data-bbox="402 306 537 338">Annonce</p> <p data-bbox="402 386 1198 611">Le pilote Windows ENA version 2.2.4 a été annulé en raison d'une dégradation potentielle des performances sur les instances EC2 de sixième génération. Nous vous recommandons de revenir à une version plus ancienne du pilote à l'aide de l'une des méthodes suivantes :</p> <ul data-bbox="402 659 1219 953" style="list-style-type: none"><li data-bbox="402 688 857 720">• Installer la version précédente<ol data-bbox="435 768 1219 953" style="list-style-type: none"><li data-bbox="435 768 1219 852">1. Téléchargez le package de la version précédente à partir du lien de ce tableau (version 2.2.3).<li data-bbox="435 873 1219 953">2. Exécutez le script install.ps1 PowerShell d'installation. <p data-bbox="435 1062 1138 1192">Pour plus de détails sur les étapes pré-installation et post-installation, consultez Activer les réseaux améliorés sur Windows.</p> <p data-bbox="435 1241 1198 1318">Utiliser Amazon EC2 Systems Manager pour effectuer une mise à jour en masse</p> <ul data-bbox="435 1367 1211 1612" style="list-style-type: none"><li data-bbox="435 1367 1211 1612">• Effectuer une mise à jour en masse via un document SSM <code>AWS-ConfigureAWSPackage</code> , avec les paramètres suivants :<ul data-bbox="496 1520 943 1612" style="list-style-type: none"><li data-bbox="496 1520 943 1556">• Nom : <code>AwsEnaNetworkDriver</code><li data-bbox="496 1577 943 1612">• Version : <code>2.2.3</code>	26 octobre 2021

Versions du pilote	Détails	Date de publication
2.2.3	<p>Nouvelle fonction</p> <ul style="list-style-type: none">• Ajoute la prise en charge des nouvelles cartes Nitro avec la mise en réseau d'une instance jusqu'à 400 Gbit/s. <p>Correctif de bogue.</p> <ul style="list-style-type: none">• Correction de la condition de concurrence entre le changement d'heure système et la requête d'heure système par le pilote ENA, ce qui provoque une détection faussement positive de la non réactivité du matériel. <p>La version 2.2.3 du pilote ENA de Windows est la dernière version qui prend en charge Windows Server 2008 R2. Les types d'instance actuellement disponibles qui utilisent ENA continueront à être pris en charge sur Windows Server 2008 R2. Les pilotes sont disponibles en téléchargement. Aucun futur type d'instance ne supportera Windows Server 2008 R2, et vous ne pouvez pas lancer, importer ou migrer des images Windows Server 2008 R2 vers de futurs types d'instance.</p>	25 mars 2021

Versions du pilote	Détails	Date de publication
2.2.2	<p>Nouvelle fonction</p> <ul style="list-style-type: none">• Permet d'interroger les indicateurs de performance des adaptateurs réseau avec CloudWatch les compteurs de performance pour les utilisateurs de Windows. <p>Correctif de bogue.</p> <ul style="list-style-type: none">• Résout les problèmes de performances sur les instances nues.	21 décembre 2020
2.2.1	<p>Nouvelle fonction</p> <ul style="list-style-type: none">• Ajoute une méthode permettant à l'hôte d'interroger l'adaptateur réseau Elastic pour les métriques des performances réseau.	1er octobre 2020

Versions du pilote	Détails	Date de publication
2.2.0	<p>Nouvelles fonctions</p> <ul style="list-style-type: none">• Ajoute la prise en charge des types de matériel de nouvelle génération.• Améliore le temps de démarrage de l'instance après la reprise suivant l'état stop-hibernate et élimine les messages d'erreur ENA faux positifs. <p>Optimisations des performances</p> <ul style="list-style-type: none">• Optimise le traitement du trafic entrant.• Améliore la gestion de la mémoire partagée dans un environnement avec peu de ressources. <p>Correctif de bogue.</p> <ul style="list-style-type: none">• Évite la panne du système lors du retrait du périphérique ENA dans le scénario rare où le pilote ne parvient pas à réinitialiser	12 août 2020
2.1.5	<p>Correctif de bogue.</p> <ul style="list-style-type: none">• Résout les échecs occasionnels d'initialisation de la carte réseau sur les instances nues.	23 Juin 2020

Versions du pilote	Détails	Date de publication
2.1.4	<p>Correctifs de bogue</p> <ul style="list-style-type: none">• Empêchent les problèmes de connectivité provoqués par des métadonnées de paquets LSO corrompus arrivant de la pile réseau.• Empêche la panne du système provoquée par une condition de concurrence rare qui se traduit par l'accès d'une mémoire de paquets déjà libérée.	25 novembre 2019
2.1.2	<p>Nouvelle fonction</p> <ul style="list-style-type: none">• Ajout de la prise en charge du rapport d'ID fournisseur pour permettre au SO de générer des UUID basés sur MAC. <p>Correctifs de bogue</p> <ul style="list-style-type: none">• Amélioration des performances de configuration du réseau DHCP pendant l'initialisation.• Calculez correctement la somme de contrôle L4 sur le trafic IPv6 entrant lorsque l'unité de transmission maximale (MTU) dépasse 4K.• Améliorations générales de la stabilité du pilote et correctifs de bogues mineurs.	4 novembre 2019

Versions du pilote	Détails	Date de publication
2.1.1	<p>Correctifs de bogue</p> <ul style="list-style-type: none">• Empêchement de la suppression des paquets TCP LSO très fragmentés provenant du système d'exploitation.• Gestion correcte du protocole ESP (Encapsulating Security Payload) dans IPSec sur les réseaux IPv6.	16 septembre 2019

Versions du pilote	Détails	Date de publication
2.1.0	<p>Le pilote Windows ENA v2.1 introduit de nouvelles capacités d'appareil ENA, accroît les performances, ajoute de nouvelles fonctionnalités et inclut plusieurs améliorations de stabilité.</p> <ul style="list-style-type: none">• Nouvelles fonctions<ul style="list-style-type: none">• Utilisez la clé de registre Windows normalisée pour la configuration des trames Jumbo.• Autorisez le paramètre d'ID VLAN via la GUI des propriétés de pilote ENA.• Flux de récupération améliorés<ul style="list-style-type: none">• Amélioration du mécanisme d'identification des défaillances.• Ajout de la prise en charge pour les paramètres de récupération réglables.• Prise en charge de 32 files d'attente d'I/O maximum pour les instances EC2 les plus récentes ayant plus de 8 vCPU.• ~90 % de réduction d'empreinte mémoire du pilote.• Optimisation des performances<ul style="list-style-type: none">• Réduction de la latence du chemin de transmission.• Prise en charge de la réception du transfert du total de contrôle.•	1 juillet 2019

Versions du pilote	Détails	Date de publication
	<p>Optimisation des performances pour un système extrêmement chargé (utilisation optimisée des mécanismes de verrouillage).</p> <ul style="list-style-type: none">• Améliorations visant à réduire l'utilisation de l'UC et à améliorer la réactivité du système face aux charges.• Correctifs de bogue<ul style="list-style-type: none">• Correction des incidents dus à une analyse non valide des en-têtes Tx non contigus.• Correction des incidents du pilote v1.5 pendant le détachement de l'interface réseau Elastic sur des instances de matériel nu.• Correction des erreurs de calcul du total de contrôle des pseudo-en-têtes LSO via IPv6.• Correction de la fuite de ressources mémoire potentielles lors de l'échec d'initialisation.• Désactivation du transfert du total de contrôle TCP/UDP pour les fragments IPv4.• Correction de la configuration VLAN. VLAN a été mal désactivé alors que la priorité VLAN uniquement aurait dû être désactivée.• Activation de l'analyse correcte des messages de pilote personnalisés par la visionneuse d'événements.•	

Versions du pilote	Détails	Date de publication
	<p>Correction de l'échec d'initialisation en raison d'un traitement non valide de l'horodatage.</p> <ul style="list-style-type: none"> • Corrigez la condition de course entre le traitement des données et la désactivation de l'appareil ENA. 	
1.5.0	<ul style="list-style-type: none"> • Amélioration de la stabilité et des correctifs de performance. • Les tampons de réception peuvent désormais être configurés sur une valeur de 8192 au maximum dans les propriétés avancées de la carte réseau ENA. • Tampons de réception par défaut de 1 000 octets. 	4 octobre 2018
1.2.3	Inclut les correctifs de fiabilité et unifie la prise en charge de Windows Server 2008 R2 via Windows Server 2016.	13 février 2018
1.0.8	Version initiale. Incluse dans les AMI pour Windows Server 2008 R2, Windows Server 2012 RTM, Windows Server 2012 R2 et Windows Server 2016.	juillet 2016

Amazon SNS peut vous notifier en cas de publication de nouvelles versions des pilotes Windows EC2. Pour vous abonner à ces notifications, utilisez la procédure suivante.

Pour s'abonner aux notifications de l'EC2

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans la barre de navigation, changez la région en US Est (Virginie du Nord), si nécessaire. Vous devez sélectionner cette région, car les notifications SNS auxquelles vous vous abonnez sont dans cette région.

3. Dans le panneau de navigation, choisissez Abonnements.
4. Choisissez Créer un abonnement.
5. Dans la boîte de dialogue Créer un abonnement, exécutez l'une des actions suivantes :
 - a. Pour TopicARN, copiez l'Amazon Resource Name (ARN) suivant :
`arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers`
 - b. Pour Protocole, choisissez Email.
 - c. Pour Point de terminaison, entrez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications.
 - d. Choisissez Créer un abonnement.
6. Vous recevrez rapidement un e-mail de confirmation. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Chaque fois que des pilotes Windows EC2 sont publiés, nous envoyons des notifications aux abonnés de la rubrique . Si vous ne souhaitez plus recevoir ces notifications, exécutez la procédure suivante pour annuler votre abonnement.

Pour se désinscrire des notifications des pilotes Windows Amazon EC2

1. Ouvrez la console Amazon SNS à partir de l'adresse <https://console.aws.amazon.com/sns/v3/home>.
2. Dans le panneau de navigation, choisissez Abonnements.
3. Cochez la case correspondant à l'abonnement, puis choisissez Actions, Supprimer des abonnements. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Améliorez les performances du réseau avec ENA Express sur vos instances EC2

ENA Express est alimenté par la technologie AWS Scalable Reliable Datagram (SRD). SRD est un protocole de transport réseau à hautes performances qui utilise le routage dynamique pour augmenter le débit et minimiser la latence de queue. Avec ENA Express, vous pouvez communiquer entre deux instances EC2 dans la même zone de disponibilité.

Avantages d'ENA Express

- Augmente la bande passante maximale qu'un seul flux peut utiliser de 5 Gbit/s à 25 Gbit/s au sein du sous-réseau, jusqu'à la limite d'instance agrégée.
- Réduit la latence du trafic réseau entre les instances EC2, en particulier pendant les périodes de forte charge réseau.
- Détecte et évite les chemins réseau encombrés.
- Gère certaines tâches directement dans la couche réseau, telles que la réorganisation des paquets du côté récepteur et la plupart des retransmissions nécessaires. Cela permet de libérer la couche d'application pour d'autres tâches.

Note

Si votre application envoie ou reçoit un volume élevé de paquets par seconde et doit optimiser la latence la plupart du temps, en particulier pendant les périodes où il n'y a pas d'encombrement sur le réseau, [Réseaux améliorés](#) peut être mieux adaptée à votre réseau.

Pendant les périodes où le trafic réseau est faible, vous pouvez remarquer une légère augmentation de la latence des paquets (quelques dizaines de microsecondes) lorsque le paquet utilise ENA Express. Pendant ces périodes, les applications qui donnent la priorité à des caractéristiques de performance réseau spécifiques peuvent bénéficier d'ENA Express de la manière suivante :

- Les processus peuvent bénéficier d'une augmentation de la bande passante à flux unique maximale de 5 Gbit/s à 25 Gbit/s au sein d'une même zone de disponibilité, jusqu'à la limite d'instances agrégée. Par exemple, si un type d'instance spécifique prend en charge jusqu'à 12,5 Gbit/s, la bande passante à flux unique est également limitée à 12,5 Gbit/s.
- Les processus qui s'exécutent depuis longtemps devraient bénéficier d'une réduction de la latence pendant les périodes d'encombrement du réseau.
- Les processus peuvent bénéficier d'une distribution plus régulière et plus standard des temps de réponse du réseau.

Conditions préalables pour les instances Linux

Pour garantir le bon fonctionnement d'ENA Express, mettez à jour les paramètres de votre instance comme suit.

- Si votre instance utilise des trames Jumbo, exécutez la commande suivante pour définir votre unité de transmission maximale (MTU) sur 8900.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- Augmentez la taille de la bague du récepteur (Rx) comme suit :

```
[ec2-user ~]$ ethtool -G device rx 8192
```

- Pour optimiser la bande passante d'ENA Express, configurez les limites de votre file d'attente TCP comme suit :

1. Définissez la limite des petites files d'attente TCP à 1 Mo ou plus. Cela augmente la quantité de données mises en file d'attente pour transmission sur un socket.

```
sudo sh -c 'echo 1048576 > /proc/sys/net/ipv4/tcp_limit_output_bytes'
```

2. Désactivez les limites de files d'attente d'octets sur le périphérique eth si elles sont activées pour votre distribution Linux. Cela augmente le nombre de données mises en file d'attente pour la transmission au niveau de la file d'attente des périphériques.

```
sudo sh -c 'for txq in /sys/class/net/eth0/queues/tx-*; do echo max > ${txq}/byte_queue_limits/limit_min; done'
```

Note

Le pilote ENA de la distribution Amazon Linux désactive les limites de files d'attente d'octets par défaut.

Fonctionnement d'ENA Express

ENA Express est alimenté par la technologie AWS Scalable Reliable Datagram (SRD). Il distribue les paquets pour chaque flux réseau sur différents chemins AWS réseau et ajuste dynamiquement la distribution lorsqu'il détecte des signes de congestion. Elle gère également la réorganisation des paquets du côté récepteur.

Pour garantir qu'ENA Express puisse gérer le trafic réseau comme prévu, les instances d'envoi et de réception, ainsi que la communication entre elles, doivent répondre à toutes les exigences suivantes :

- Les types d'instance d'envoi et de réception sont pris en charge. Consultez la table [Types d'instance pris en charge pour ENA Express](#) pour plus d'informations.
- ENA Express doit être configuré pour les instances d'envoi et de réception. S'il existe des différences de configuration, vous pouvez vous retrouver dans des situations où le trafic passe par défaut à une transmission ENA standard. Le scénario suivant montre ce qui peut se passer.

Scénario : différences de configuration

Instance	ENA Express activé	UDP utilise ENA Express
Instance 1	Oui	Oui
Instance 2	Oui	Non

Dans ce cas, le trafic TCP entre les deux instances peut utiliser ENA Express, car les deux instances l'ont activé. Toutefois, étant donné que l'une des instances n'utilise pas ENA Express pour le trafic UDP, la communication entre ces deux instances via UDP utilise une transmission ENA standard.

- Les instances d'envoi et de réception doivent s'exécuter dans la même zone de disponibilité.
- Le chemin réseau entre les instances ne doit pas inclure de boîtiers intergiciels. ENA Express ne prend actuellement pas en charge les boîtiers intergiciels.
- (Instances Linux uniquement) Pour utiliser tout le potentiel de bande passante, utilisez la version 2.2.9 ou supérieure du pilote.
- (Instances Linux uniquement) Pour produire des métriques, utilisez la version 2.8 ou supérieure du pilote.

Si l'une des exigences n'est pas satisfaite, les instances utilisent le protocole TCP/UDP standard, mais sans SRD, pour communiquer.

Pour vous assurer que le pilote réseau de votre instance est configuré pour des performances optimales, veuillez consulter les bonnes pratiques recommandées pour les pilotes ENA. Ces bonnes pratiques s'appliquent également à ENA Express. Pour plus d'informations, consultez le [guide des meilleures pratiques et d'optimisation des performances des pilotes Linux ENA](#) sur le GitHub site Web.

Note

Amazon EC2 fait référence à la relation entre une instance et une interface réseau qui lui est attachée en tant qu'attachement. Les paramètres ENA Express s'appliquent à l'attachement. Si l'interface réseau est détachée de l'instance, l'attachement n'existe plus et les paramètres ENA Express qui s'y appliquaient ne sont plus en vigueur. Il en va de même lorsqu'une instance est résiliée, même si l'interface réseau est conservée.

Types d'instance pris en charge pour ENA Express

Les onglets suivants indiquent les types d'instances compatibles avec ENA Express.

General purpose

Type d'instance	Architecture
m6a.12xlarge	x86_64
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64
m6i.metal	x86_64

Type d'instance	Architecture
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64
m6id.metal	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64

Compute optimized

Type d'instance	Architecture
c6a.12xlarge	x86_64
c6a.16xlarge	x86_64
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64
c6a.48xlarge	x86_64
c6a.metal	x86_64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64
c6id.metal	x86_64

Type d'instance	Architecture
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64
c7gd.metal	arm64
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24x1	x86_64
c7i.metal-48x1	x86_64

Memory optimized

Type d'instance	Architecture
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64
r6a.48xlarge	x86_64

Type d'instance	Architecture
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64
r6id.32xlarge	x86_64
r6id.metal	x86_64
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64
r7i.12xlarge	x86_64

Type d'instance	Architecture
r7i.16xlarge	x86_64
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64
r7i.metal-24x1	x86_64
r7i.metal-48x1	x86_64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64

Accelerated computing

Type d'instance	Architecture
g6.48xlarge	x86_64

Storage optimized

Type d'instance	Architecture
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64
i4i.32xlarge	x86_64
i4i.metal	x86_64
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Répertorier et afficher les paramètres ENA Express

Cette section explique comment répertorier et afficher les informations ENA Express à partir de AWS Management Console ou de AWS CLI. Pour de plus amples informations, choisissez l'onglet qui correspond à la méthode que vous allez utiliser.

Console

Cet onglet explique comment trouver des informations sur vos paramètres ENA Express actuels et comment consulter la prise en charge des types d'instance dans la AWS Management Console.

Afficher la prise en charge de type d'instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, choisissez Instance Types (Types d'instance).
3. Sélectionnez un type d'instance pour afficher les détails de cette instance. Vous pouvez cliquer sur le lien Instance type (Type d'instance) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste pour afficher les détails dans le volet détaillé en bas de la page.
4. Dans l'onglet Networking (Réseau) ou dans cette section de la page détaillée, la prise en charge d'ENA Express affiche une valeur vraie ou fausse pour indiquer si le type d'instance prend en charge cette fonctionnalité.

Afficher les paramètres à partir de la liste de l'interface réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez une interface réseau pour afficher les détails de cette instance. Vous pouvez cliquer sur le lien Network interface ID (ID d'interface réseau) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste pour afficher les détails dans le volet détaillé en bas de la page.
4. Dans la section Network interface attachment (Attachement interface réseau) de l'onglet Details (Détails) ou de la page de détails, passez en revue les paramètres ENA Express et ENA Express UDP.

Afficher les paramètres à partir d'instances

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, sélectionnez instances.
3. Sélectionnez une instance pour afficher les détails de cette instance. Vous pouvez cliquer sur le lien Instance ID (ID d'instance) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste pour afficher les détails dans le volet détaillé en bas de la page.

4. Dans la section Network interfaces (Interfaces réseau) de l'onglet Networking (Réseau), faites défiler l'écran vers la droite pour passer en revue les paramètres ENA Express et ENA Express UDP.

AWS CLI

Cet onglet explique comment trouver des informations sur vos paramètres ENA Express actuels et comment consulter la prise en charge des types d'instance dans la AWS CLI.

Décrire les types d'instance

Pour plus d'informations sur les paramètres de type d'instance pour un type d'instance spécifique, exécutez la [describe-instance-types](#) commande dans le AWS CLI et remplacez le type d'instance comme suit :

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-types m6i.metal
{
  "InstanceTypes": [
    {
      "InstanceType": "m6i.metal",
      "CurrentGeneration": true,
      ...
    },
    "NetworkInfo": {
      ...
      "EnaSrdSupported": true
    },
    ...
  ]
}
```

Décrire des instances

Pour plus d'informations sur la configuration d'ENA Express pour les instances spécifiées, exécutez la [describe-instances](#) commande dans le AWS CLI, comme suit. Cet exemple de commande renvoie une liste des configurations ENA Express pour les interfaces réseau associées à chacune des instances en cours d'exécution spécifiées par le `--instance-ids` paramètre.

```
[ec2-user ~]$ aws ec2 describe-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7 --query 'Reservations[*].Instances[*].[InstanceId, NetworkInterfaces[*].Attachment.EnaSrdSpecification]'
```

```
[
  [
    "i-1234567890abcdef0",
    [
      {
        "EnaSrdEnabled": true,
        "EnaSrdUdpSpecification": {
          "EnaSrdUdpEnabled": false
        }
      }
    ]
  ],
  [
    [
      "i-0598c7d356eba48d7",
      [
        {
          "EnaSrdEnabled": true,
          "EnaSrdUdpSpecification": {
            "EnaSrdUdpEnabled": false
          }
        }
      ]
    ]
  ]
]
```

Décrire les interfaces réseau

Pour plus d'informations sur les paramètres ENA Express d'une interface réseau, exécutez la [describe-network-interfaces](#) commande AWS CLI comme suit :

```
[ec2-user ~]$ aws ec2 describe-network-interfaces
```

```
{
  "NetworkInterfaces": [
    {
      "Association": {
        ....IPs, DNS...
      },
```

```

"Attachment": {
  "AttachTime": "2022-11-17T09:04:28+00:00",
  "AttachmentId": "eni-attach-0ab1c23456d78e9f0",
  "DeleteOnTermination": true,
  "DeviceIndex": 0,
  "NetworkCardIndex": 0,
  "InstanceId": "i-1234567890abcdef0",
  "InstanceOwnerId": "111122223333",
  "Status": "attached",
  "EnaSrdSpecification": {
    "EnaSrdEnabled": true,
    "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": true
    }
  }
},
...
"NetworkInterfaceId": "eni-1234567890abcdef0",
"OwnerId": "111122223333",
...
}
]
}

```

PowerShell

Cet onglet explique comment trouver des informations sur vos paramètres ENA Express actuels et comment consulter la prise en charge des types d'instance à l'aide de PowerShell.

Décrire les types d'instance

Pour plus d'informations sur les paramètres de type d'instance pour un type d'instance spécifique, exécutez le [Get-EC2InstanceType Cmdlet](#) avec les outils pour PowerShell et remplacez le type d'instance comme suit :

```

PS C:\> Get-EC2InstanceType -InstanceType m6i.metal | `
Select-Object `
    InstanceType,
    CurrentGeneration,
    @{Name = 'EnaSrdSupported'; Expression = { $_.NetworkInfo.EnaSrdSupported } } |
Format-List

```

```

InstanceType      : m6i.metal
CurrentGeneration : True
EnaSrdSupported   : True

```

Si ENA Express est activé, une valeur de True est renvoyée.

Décrire les interfaces réseau

Pour plus d'informations sur les paramètres ENA Express d'une interface réseau, exécutez le [Get-EC2NetworkInterface Cmdlet](#) à l'aide PowerShell des outils suivants :

```

PS C:\> Get-EC2NetworkInterface -NetworkInterfaceId eni-0d1234e5f6a78901b | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
{ $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
{ $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
    @{Name = 'EnaSrdUdpEnabled'; Expression =
{ $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }

Association      :
NetworkInterfaceId : eni-0d1234e5f6a78901b
OwnerId          : 111122223333
AttachTime       : 6/11/2022 1:13:11 AM
AttachmentId     : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
NetworkCardIndex : 0
InstanceId       : i-0d1234e5f6a78901b
InstanceOwnerId  : 111122223333
Status          : attached
EnaSrdEnabled    : True
EnaSrdUdpEnabled : False

```

Configurer les paramètres ENA Express

Vous pouvez configurer ENA Express pour les types d'instance EC2 pris en charge sans avoir à installer de logiciel supplémentaire.

Cette section explique comment configurer ENA Express depuis AWS Management Console ou depuis le AWS CLI. Pour de plus amples informations, choisissez l'onglet qui correspond à la méthode que vous allez utiliser.

Console

Cet onglet explique comment gérer les paramètres ENA Express pour les interfaces réseau associées à une instance.

Gestion d'ENA Express à partir de la liste des interfaces réseau

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez une interface réseau qui doit être attachée à une instance. Vous pouvez cliquer sur le lien Network interface ID (ID d'interface réseau) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste.
4. Choisissez Manage ENA Express (Gérer ENA Express) dans le menu Action en haut à droite de la page. Cela ouvre la boîte de dialogue Manage ENA Express (Gestion d'ENA Express), qui affiche l'ID de l'interface réseau sélectionnée et les paramètres actuels.

Note

Si l'interface réseau que vous avez sélectionnée n'est pas associée à une instance, cette action n'apparaît pas dans le menu.

5. Pour utiliser ENA Express, cochez la case Enable (Activer).
6. Lorsque ENA Express est activé, vous pouvez configurer les paramètres UDP. Pour utiliser ENA Express UDP, cochez la case Enable (Activer).
7. Pour enregistrer vos paramètres, choisissez Save (Enregistrer).

Gérer ENA Express à partir de la liste d'instances

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation de gauche, sélectionnez instances.
3. Sélectionnez l'instance que vous voulez gérer. Vous pouvez choisir Instance ID (ID d'instance) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste.
4. Sélectionnez Network interface (Interface réseau) pour configurer pour votre instance.
5. Choisissez Manage ENA Express (Gérer ENA Express) dans le menu Action en haut à droite de la page.
6. Pour configurer ENA Express pour une interface réseau attachée à votre instance, sélectionnez-la dans la liste Network interface (Interface réseau).
7. Pour utiliser ENA Express pour l'attachement de l'interface réseau sélectionné, cochez la case Enable (Activer).
8. Lorsque ENA Express est activé, vous pouvez configurer les paramètres UDP. Pour utiliser ENA Express UDP, cochez la case Enable (Activer).
9. Pour enregistrer vos paramètres, choisissez Save (Enregistrer).

Configurer ENA Express lorsque vous attachez une interface réseau à une instance EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, choisissez Network Interfaces (Interfaces réseau).
3. Sélectionnez une interface réseau qui n'est pas attachée à une instance (l'état est Available (Disponible)). Vous pouvez cliquer sur le lien Network interface ID (ID d'interface réseau) pour ouvrir la page détaillée ou cocher la case sur le côté gauche de la liste.
4. Sélectionnez l'instance avec laquelle vous souhaitez effectuer l'attachement.
5. Pour utiliser ENA Express après avoir attaché l'interface réseau à l'instance, cochez la case Enable (Activer).
6. Lorsque ENA Express est activé, vous pouvez configurer les paramètres UDP. Pour utiliser ENA Express UDP, cochez la case Enable (Activer).
7. Pour attacher l'interface réseau à l'instance et enregistrer vos paramètres ENA Express, choisissez Attach (Attacher).

AWS CLI

Cet onglet explique comment configurer les paramètres ENA Express dans AWS CLI.

Configurer ENA Express lorsque vous attachez une interface réseau

Pour configurer ENA Express lorsque vous attachez une interface réseau à une instance, exécutez la [attach-network-interface](#) commande dans le AWS CLI, comme indiqué dans les exemples suivants :

Exemple 1 : Utiliser ENA Express pour le trafic TCP, mais pas pour le trafic UDP

Dans cet exemple, nous configurons `EnaSrdEnabled` comme `true` et nous autorisons `EnaSrdUdpEnabled` par défaut sur `false`.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-srd-specification 'EnaSrdEnabled=true'
{
  "AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Exemple 2 : Utiliser ENA Express à la fois pour le trafic TCP et le trafic UDP

Dans cet exemple, nous configurons `EnaSrdEnabled` et `EnaSrdUdpEnabled` comme `true`.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-srd-specification 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
{
  "AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Mettre à jour les paramètres ENA Express pour l'attachement de votre interface réseau

Pour mettre à jour les paramètres ENA Express pour une interface réseau attachée à une instance, exécutez la [modify-network-interface-attribute](#) commande dans le AWS CLI, comme indiqué dans les exemples suivants :

Exemple 1 : Utiliser ENA Express pour le trafic TCP, mais pas pour le trafic UDP

Dans cet exemple, nous configurons `EnaSrdEnabled` comme `true`, et nous autorisons `EnaSrdUdpEnabled` par défaut sur `false` si cela n'a jamais été défini auparavant.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --network-interface-id eni-0123f4567890a1b23 --ena-srd-specification 'EnaSrdEnabled=true'
```

Exemple 2 : Utiliser ENA Express à la fois pour le trafic TCP et le trafic UDP

Dans cet exemple, nous configurons `EnaSrdEnabled` et `EnaSrdUdpEnabled` comme `true`.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --  
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification  
'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Exemple 3 : arrêter d'utiliser ENA Express pour le trafic UDP

Dans cet exemple, nous configurons `EnaSrdUdpEnabled` comme `false`.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --  
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification  
'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

Cet onglet explique comment configurer les paramètres ENA Express à l'aide de PowerShell.

Configurer ENA Express lorsque vous attachez une interface réseau

Pour configurer les paramètres ENA Express pour une interface réseau, exécutez le [Add-EC2NetworkInterface Cmdlet](#) avec les outils pour, PowerShell comme indiqué dans les exemples suivants :

Exemple 1 : Utiliser ENA Express pour le trafic TCP, mais pas pour le trafic UDP

Dans cet exemple, nous configurons `EnaSrdEnabled` comme `true` et nous autorisons `EnaSrdUdpEnabled` par défaut sur `false`.

```
PS C:\> Add-EC2NetworkInterface `   
-NetworkInterfaceId eni-0123f4567890a1b23 `   
-InstanceId i-0f1a234b5cd67e890 `   
-DeviceIndex 1 `   
-EnaSrdSpecification_EnaSrdEnabled $true   
  
eni-attach-012c3d45e678f9012
```

Exemple 2 : Utiliser ENA Express à la fois pour le trafic TCP et le trafic UDP

Dans cet exemple, nous configurons `EnaSrdEnabled` et `EnaSrdUdpEnabled` comme `true`.

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdUdpSpecification_EnaSrdUdpEnabled $true

eni-attach-012c3d45e678f9012
```

Mettre à jour les paramètres ENA Express pour l'attachement de votre interface réseau

Pour mettre à jour les paramètres ENA Express pour une interface réseau attachée à une instance, exécutez la [Add-EC2NetworkInterface Cmdlet](#) commande dans les outils pour PowerShell, comme indiqué dans les exemples suivants :

Exemple 1 : Utiliser ENA Express pour le trafic TCP, mais pas pour le trafic UDP

Dans cet exemple, nous configurons `EnaSrdEnabled` comme `true`, et nous autorisons `EnaSrdUdpEnabled` par défaut sur `false` si cela n'a jamais été défini auparavant.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
    { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
    { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Exemple 2 : Utiliser ENA Express à la fois pour le trafic TCP et le trafic UDP

Dans cet exemple, nous configurons `EnaSrdEnabled` et `EnaSrdUdpEnabled` comme `true`.

```

PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
    { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
    { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : True

```

Exemple 3 : arrêter d'utiliser ENA Express pour le trafic UDP

Dans cet exemple, nous configurons `EnaSrdUdpEnabled` comme `false`.

```

PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
    { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
    { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False

```

Configurer ENA Express au lancement

Vous pouvez utiliser l'une des méthodes suivantes afin de configurer ENA Express pour une AMI lorsque vous lancez une instance depuis l' AWS Management Console.

- Vous pouvez configurer ENA Express pour votre AMI lorsque vous lancez une instance à l'aide de l'assistant de lancement d'instance. Pour plus de détails sur la configuration, consultez la rubrique Configuration réseau avancée dans les [Paramètres réseau](#) pour l'assistant de lancement d'instance.
- Vous pouvez configurer ENA Express pour votre AMI lorsque vous utilisez un modèle de lancement. Pour plus d'informations sur la configuration des modèles de lancement, consultez la rubrique Configuration réseau avancée dans les [Paramètres réseau](#) pour les modèles de lancement.

Surveiller les performances ENA Express

Après avoir activé ENA Express pour les attachements de l'interface réseau à la fois sur l'instance d'envoi et sur l'instance de réception, vous pouvez utiliser les métriques ENA Express pour vous assurer que vos instances tirent pleinement parti des améliorations de performances apportées par la technologie SRD.

Pour consulter la liste des mesures filtrées pour ENA Express, exécutez la commande `ethtool` suivante pour votre interface réseau (présentée ici en tant que `eth0`) :

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
ena_srd_mode: 0
ena_srd_tx_pkts: 0
ena_srd_eligible_tx_pkts: 0
ena_srd_rx_pkts: 0
ena_srd_resource_utilization: 0
```

Vérifier les paramètres ENA Express pour une instance

Pour vérifier les paramètres actuels d'ENA Express pour l'attachement à l'interface réseau de votre instance, exécutez la commande `ethtool` pour répertorier les métriques ENA Express et prenez note de la valeur de la métrique `ena_srd_mode`. Les valeurs sont les suivantes :

- 0 = ENA Express désactivé, UDP désactivé
- 1 = ENA Express activé, UDP désactivé
- 2 = ENA Express désactivé, UDP activé

Note

Cela se produit uniquement lorsque ENA Express a été initialement activé et que UDP a été configuré pour l'utiliser. La valeur précédente est conservée pour le trafic UDP.

- 3 = ENA Express activé, UDP activé

Une fois que vous avez activé ENA Express pour l'attachement d'interface réseau sur une instance, l'instance d'envoi initie la communication avec l'instance de réception et SRD détecte si ENA Express fonctionne à la fois sur l'instance d'envoi et l'instance de réception. Si ENA Express fonctionne, la communication peut utiliser la transmission SRD. Si ENA Express ne fonctionne pas, la communication revient à la transmission ENA standard. Pour vérifier si la transmission de paquets utilise le SRD, vous pouvez comparer le nombre de paquets éligibles (métrique `ena_srd_eligible_tx_pkts`) par rapport au nombre de paquets SRD transmis (métrique `ena_srd_tx_pkts`) au cours d'une période donnée.

Vous pouvez surveiller l'utilisation de vos ressources SRD à l'aide de la métrique `ena_srd_resource_utilization`. Si votre instance est sur le point d'épuiser ses ressources SRD, vous savez qu'il est temps de la faire monter en puissance.

Pour plus d'informations sur les métriques ENA Express, veuillez consulter [Métriques pour ENA Express](#).

Réglez les performances pour les paramètres ENA Express

Pour vérifier la configuration de votre instance Linux afin d'optimiser les performances d'ENA Express, vous pouvez exécuter le script suivant, disponible sur le GitHub référentiel Amazon :

<https://github.com/amzn/amzn-ec2-ena-utilities/blob/main/ena-express/check-ena-express-settings.sh>

Le script exécute une série de tests et suggère les modifications de configuration recommandées et requises.

Activez une mise en réseau améliorée avec l'interface Intel 82599 VF sur vos instances EC2

Amazon EC2 fournit des fonctionnalités de mise en réseau améliorée via l'interface Intel 82599 VF, qui utilise le pilote Intel `ixgbevf`.

Table des matières

- [Prérequis](#)
- [Vérifiez que le pilote est installé](#)
- [Tester l'activation de réseaux améliorés](#)
- [Activer les réseaux améliorés sur une instance](#)
- [Résoudre les problèmes de connectivité](#)

Prérequis

Pour vous préparer à la mise en réseau améliorée à l'aide de l'interface Intel 82599 VF, configurez l'instance comme suit :

- Effectuez votre sélection parmi les types d'instances pris en charge suivants : C3, C4, D2, I2, M4 (à l'exception de m4.16xlarge) et R3.
- Vérifiez que l'instance a une connectivité Internet.
- Si l'instance comporte des données importantes que vous souhaitez conserver, vous devez les sauvegarder maintenant en créant une AMI à partir de votre instance. La mise à jour des noyaux et des modules noyau, ainsi que l'activation de l'attribut `sriovNetSupport`, peuvent rendre les instances incompatibles ou les systèmes d'exploitation inaccessibles. Si cela se produit et que vous disposez d'une sauvegarde récente, vos données continueront d'être conservées.
- Instances Linux : lancez l'instance depuis une AMI HVM à l'aide de la version 2.6.32 ou ultérieure du noyau Linux. Les AMI HVM Amazon Linux les plus récentes disposent des attributs et des modules requis pour la mise en réseau améliorée. Par conséquent, si vous lancez une instance avec prise en charge des réseaux améliorés et basée sur Amazon EBS à l'aide d'une AMI HVM Amazon Linux active, les réseaux améliorés sont déjà activés pour votre instance.

Warning

La mise en réseau améliorée n'est prise en charge que pour les instances HVM. L'activation de la mise en réseau améliorée avec une instance de paravirtualisation peut la rendre inaccessible. La définition de cet attribut sans le module ou la version de module approprié peut rendre votre instance inaccessible.

- Instances Windows : lancez l'instance à partir d'une AMI HVM 64 bits. Vous ne pouvez pas activer la mise en réseau améliorée sur Windows Server 2008. La mise en réseau améliorée est déjà activée pour les AMI Windows Server 2012 R2 et Windows Server 2016 et versions ultérieures.

Windows Server 2012 R2 inclut le pilote Intel 1.0.15.3, et nous vous recommandons de le mettre à jour à l'aide de l'utilitaire Pnputil.exe afin d'obtenir la version la plus récente.

- [AWS CloudShell](#) Utilisez-le depuis ou installez et configurez le [AWS CLI](#) ou [AWS Tools for Windows PowerShell](#) sur n'importe quel ordinateur de votre choix, de préférence sur votre ordinateur de bureau ou portable local. AWS Management Console Pour plus d'informations, consultez la section [Accès à Amazon EC2](#) du [Guide de l'utilisateur AWS CloudShell](#). La gestion de la mise en réseau améliorée n'est pas possible à partir de la console Amazon EC2.

Vérifiez que le pilote est installé

Vérifiez que le pilote est installé sur votre instance.

pilote d'interface réseau Linux

Utilisez la commande suivante pour vérifier que le module est utilisé sur une interface particulière, en remplaçant le nom de l'interface par celui que vous voulez contrôler. Si vous utilisez une seule interface (par défaut), ce sera `eth0`. Si le système d'exploitation prend en charge les [noms de réseau prévisibles](#), il peut s'agir d'un nom tel que `ens5`.

Dans l'exemple suivant, le module `ixgbevf` n'est pas chargé, car le pilote affiché est `vif`.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Dans cet exemple, le module `ixgbevf` est chargé. La mise en réseau améliorée est correctement configurée pour cette instance.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
```

```
supports-statistics: yes
supports-test: yes
supports-EEPROM-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Adaptateur réseau Windows

Pour vérifier que le pilote est installé, connectez-vous à votre instance et ouvrez le Gestionnaire de périphériques. La mention « Intel(R) 82599 Virtual Function » doit apparaître sous Cartes réseau.

Tester l'activation de réseaux améliorés

Vérifiez que l'`sriovNetSupport` attribut est défini.

Attribut d'instance (sriovNetSupport)

Pour vérifier si l'attribut de mise en réseau améliorée `sriovNetSupport` est défini sur une instance, utilisez l'une des commandes suivantes. Si l'attribut est défini, la valeur est `simple`.

- [describe-instance-attribute](#) (AWS CLI) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute
sriovNetSupport
```

- [Get-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute sriovNetSupport
```

Attribut d'image (sriovNetSupport)

Pour vérifier si l'`sriovNetSupport` attribut réseau amélioré est déjà défini pour une AMI, utilisez l'une des commandes suivantes. Si l'attribut est défini, la valeur est `simple`.

- [describe-images](#) (AWS CLI)

```
aws ec2 describe-images --image-id ami_id --query "Images[].SriovNetSupport"
```

- [Get-EC2Image](#) (AWS Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami-id).SriovNetSupport
```

Activer les réseaux améliorés sur une instance

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Warning

Il n'existe aucun moyen de désactiver l'attribut de mise en réseau améliorée une fois que vous l'avez activé.

Amazon Linux

Les AMI HVM Amazon Linux les plus récentes disposent du module `ixgbevf` et de l'attribut `srhovNetSupport` requis pour la mise en réseau améliorée. Par conséquent, si vous lancez un type d'instance à l'aide d'une AMI HVM Amazon Linux actuelle, la mise en réseau améliorée est déjà activée pour votre instance. Pour plus d'informations, consultez [Tester l'activation de réseaux améliorés](#).

Si vous avez lancé votre instance avec une version d'Amazon Linux AMI plus ancienne et que la mise en réseau améliorée n'est pas activée sur cette dernière, utilisez le procédure suivante pour l'activer.

Pour activer la mise en réseau améliorée

1. Connectez-vous à votre instance.
2. Depuis l'instance, exécutez la commande suivante pour mettre à jour votre instance avec le noyau et les modules noyau les plus récents, y compris `ixgbevf` :

```
[ec2-user ~]$ sudo yum update
```

3. Depuis votre ordinateur local, réinitialisez votre instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [reboot-instances](#) (AWS CLI), [Restart-EC2Instance](#) (AWS Tools for Windows PowerShell).
4. Connectez-vous à nouveau à votre instance et vérifiez que le module `ixgbevf` est installé et possède la version minimale recommandée à l'aide de la commande `modinfo ixgbevf` depuis [Tester l'activation de réseaux améliorés](#).
5. [Instance basée sur EBS] À partir de votre ordinateur local, arrêtez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [stop-instances](#) (AWS CLI),

[Stop-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

[Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Vous devez utiliser cette procédure : [Pour activer la mise en réseau améliorée \(instances basées sur le stockage d'instance\)](#).

6. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:

AWS CLI

[modify-instance-attribute](#) (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support simple
```

PowerShell

[Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

7. (Facultatif) Créez une AMI à partir de l'instance, comme décrit dans [Création d'une AMI basée sur Amazon EBS](#). L'AMI hérite de l'attribut de mise en réseau améliorée de l'instance. Par conséquent, vous pouvez utiliser cet AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.
8. Depuis votre ordinateur local, démarrez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [start-instances](#) (AWS CLI), [Start-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.
9. Connectez-vous à votre instance et vérifiez que le module `ixgbevf` est installé et chargé sur votre interface réseau à l'aide de la commande `ethtool -i ethn` depuis [Tester l'activation de réseaux améliorés](#).

Pour activer la mise en réseau améliorée (instances basées sur le stockage d'instance)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez une nouvelle AMI comme décrit dans [Créer une AMI Linux basée sur le stockage d'instance](#), en veillant à activer l'attribut de mise en réseau améliorée lors de l'enregistrement de l'AMI.

AWS CLI

[register-image](#) (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

[Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Avant de commencer, [vérifiez si la mise en réseau améliorée est déjà activée](#) sur votre instance.

Les AMI HVM Ubuntu Quick Start comprennent les pilotes nécessaires pour la mise en réseau améliorée. Si vous disposez d'une version du fichier `ixgbev` antérieure à 2.16.4, vous pouvez installer le package noyau `linux-aws` pour obtenir les pilotes de mise en réseau améliorée les plus récents.

La procédure suivante fournit les étapes générales pour la compilation du module `ixgbev` sur une instance Ubuntu.

Pour installer le package du noyau **linux-aws**

1. Connectez-vous à votre instance.
2. Mettez à jour le cache du package et les packages.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

⚠ Important

Si, lors d'une mise à jour, vous êtes invité à installer grub, utilisez `/dev/xvda` pour installer grub, puis choisissez de conserver la version actuelle de `/boot/grub/menu.lst`.

Autres distributions Linux

Avant de commencer, [vérifiez si la mise en réseau améliorée est déjà activée](#) sur votre instance. Les dernières AMI HVM Quick Start comprennent les pilotes nécessaires pour la mise en réseau améliorée. Vous n'avez donc pas besoin d'effectuer des étapes supplémentaires.

La procédure suivante fournit les étapes générales pour si vous devez activer la mise en réseau améliorée avec l'interface Intel 82599 VF sur une distribution Linux autre qu'Amazon Linux ou Ubuntu. Pour plus d'informations, telles que la syntaxe détaillée des commandes, les emplacements de fichier ou la prise en charge des packages et des outils, consultez la documentation spécifique de votre distribution Linux.

Pour activer la mise en réseau améliorée sur Linux

1. Connectez-vous à votre instance.
2. Téléchargez la source pour le module `ixgbevf` sur votre instance depuis Sourceforge, à l'adresse <https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/>.

Les versions d'`ixgbevf` antérieures à 2.16.4, notamment la 2.14.2, ne sont pas générées correctement sur certaines distributions Linux, y compris certaines versions d'Ubuntu.

3. Compilez et installez le module `ixgbevf` sur votre instance.

⚠ Warning

Si vous compilez le module `ixgbevf` pour votre noyau actuel, puis mettez à niveau le noyau sans générer à nouveau le pilote du nouveau noyau, il se peut que votre système retourne au module `ixgbevf` spécifique à la distribution lors du prochain redémarrage. Cela peut rendre votre système inaccessible si la version propre à la distribution n'est pas compatible avec la mise en réseau améliorée.

4. Exécutez la commande `sudo depmod` pour mettre à jour les dépendances du module.

5. Mettez à jour `initramfs` sur votre instance pour garantir que le nouveau module se charge au démarrage.
6. Déterminez si par défaut votre système utilise des noms d'interface réseau prévisibles. Les systèmes qui utilisent `systemd` ou `udev` version 197 ou supérieure peuvent renommer les périphériques Ethernet et ne garantissent pas qu'une seule interface réseau sera nommée `eth0`. Ce comportement peut entraîner des problèmes de connexion à votre instance. Pour plus d'informations et pour voir les autres options de configuration, consultez la section sur les [noms d'interface réseau prévisibles](#) sur le site web de freedesktop.org.
 - a. Vous pouvez vérifier les versions `systemd` ou `udev` sur les systèmes RPM en utilisant la commande suivante :

```
[ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|udev-[0-9]\+'
systemd-208-11.el7_0.2.x86_64
```

Dans l'exemple Red Hat Enterprise Linux 7 ci-dessus, la version `systemd` est 208, de sorte que les noms d'interface réseau prévisibles doivent être désactivés.

- b. Désactivez les noms d'interface réseau prévisibles en ajoutant l'option `net.ifnames=0` à la ligne `GRUB_CMDLINE_LINUX` dans `/etc/default/grub`.

```
[ec2-user ~]$ sudo sed -i '/^GRUB_CMDLINE_LINUX/s/\ "$/\ net.ifnames=0"/' /etc/default/grub
```

- c. Générez à nouveau le fichier de configuration `grub`.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Instance basée sur EBS] À partir de votre ordinateur local, arrêtez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [stop-instances](#) (AWS CLI/AWS CloudShell), [Stop-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

[Instance basée sur le stockage d'instance] Vous ne pouvez pas arrêter l'instance pour modifier l'attribut. Vous devez utiliser cette procédure : [Pour activer les réseaux améliorés \(instances basées sur le stockage d'instance\)](#).

8. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:

AWS CLI

[modify-instance-attribute](#) (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support simple
```

PowerShell

[Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

9. (Facultatif) Créez une AMI à partir de l'instance, comme décrit dans [Création d'une AMI basée sur Amazon EBS](#). L'AMI hérite de l'attribut de mise en réseau améliorée de l'instance. Par conséquent, vous pouvez utiliser cet AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.

Si le système d'exploitation de votre instance contient un fichier `/etc/udev/rules.d/70-persistent-net.rules`, vous devez le supprimer avant de créer l'AMI. Ce fichier contient l'adresse MAC de la carte Ethernet de l'instance d'origine. Si une autre instance démarre avec ce fichier, le système d'exploitation ne pourra pas trouver le périphérique et il se peut qu'`eth0` échoue, entraînant des problèmes de démarrage. Le fichier est à nouveau généré au cycle de démarrage suivant et les instances lancées depuis l'AMI créent leur propre version du fichier.

10. Depuis votre ordinateur local, démarrez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [start-instances](#) (AWS CLI), [Start-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.
11. (Facultatif) Connectez-vous à votre instance et vérifiez que le module est installé.

Pour activer les réseaux améliorés (instances basées sur le stockage d'instance)

Suivez la procédure précédente jusqu'à l'étape à laquelle vous avez arrêté l'instance. Créez une nouvelle AMI comme décrit dans [Créer une AMI Linux basée sur le stockage d'instance](#), en veillant à activer l'attribut de mise en réseau améliorée lors de l'enregistrement de l'AMI.

AWS CLI

[register-image](#) (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

[Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Si vous avez lancé votre instance et qu'elle n'a pas la mise en réseau déjà activée, vous devez télécharger et installer le pilote de la carte réseau requis sur votre instance, puis définir l'attribut d'instance `sriovNetSupport` pour activer la mise en réseau améliorée. Vous ne pouvez activer cet attribut que sur les types d'instance pris en charge. Pour plus d'informations, consultez [Prise en charge de la mise en réseau améliorée](#).

Important

Pour consulter les dernières mises à jour des pilotes dans les AMI Windows, consultez [l'historique des versions des AMI Windows](#) dans le Guide de référence des AMI AWS Windows.

Pour activer la mise en réseau améliorée

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. [Windows Server 2016 et versions ultérieures] Exécutez le PowerShell script de lancement EC2 suivant pour configurer l'instance une fois le pilote installé.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -  
Schedule
```

⚠ Important

Le mot de passe de l'administrateur sera réinitialisé lorsque vous activerez le script d'initialisation de l'instance EC2 Launch. Vous pouvez modifier le fichier de configuration pour désactiver la réinitialisation du mot de passe administrateur en le spécifiant dans les paramètres des tâches d'initialisation.

3. À partir de l'instance, téléchargez le pilote de la carte réseau Intel adapté à votre système d'exploitation :

- Windows Server 2022

Visitez la [page de téléchargement](#) et téléchargez `Wired_driver_<version>_x64.zip`.

- Windows Server 2019 notamment pour Server version 1809 ou ultérieure*

Visitez la [page de téléchargement](#) et téléchargez `Wired_driver_<version>_x64.zip`.

- Windows Server 2016 notamment pour Server version 1803 ou antérieure*

Visitez la [page de téléchargement](#) et téléchargez `Wired_driver_<version>_x64.zip`.

- Windows Server 2012 R2

Visitez la [page de téléchargement](#) et téléchargez `Wired_driver_<version>_x64.zip`.

- Windows Server 2012

Visitez la [page de téléchargement](#) et téléchargez `Wired_driver_<version>_x64.zip`.

- Windows Server 2008 R2

Visitez la [page de téléchargement](#) et téléchargez `PROWinx64Legacy.exe`.

*Les versions 1803 et antérieures de Server, ainsi que les versions 1809 et ultérieures, ne sont pas spécifiquement traitées dans les pages relatives aux pilotes et logiciels Intel.

4. Installez le pilote de la carte réseau Intel adapté à votre système d'exploitation :

- Windows Server 2008 R2

1. Dans le dossier Téléchargements, localisez le fichier `PROWinx64Legacy.exe` et renommez-le `PROWinx64Legacy.zip`.

2. Extrayez le contenu du fichier `PROWinx64Legacy.zip`.

3. Ouvrez la ligne de commande, accédez au dossier extrait et exécutez la commande suivante pour utiliser l'utilitaire `pnputil` afin d'ajouter et d'installer le fichier INF dans le magasin de pilotes.

```
C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
```

- Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 et Windows Server 2012
 1. Dans le dossier Téléchargements, extrayez le contenu du fichier `Wired_driver_version_x64.zip`.
 2. Dans le dossier extrait, recherchez le fichier `Wired_driver_version_x64.exe` et renommez-le `Wired_driver_version_x64.zip`.
 3. Extrayez le contenu du fichier `Wired_driver_version_x64.zip`.
 4. Ouvrez la ligne de commande, accédez au dossier extrait et exécutez l'une des commandes suivantes pour utiliser l'utilitaire `pnputil` pour ajouter et installer le fichier INF dans le magasin de pilotes.

- Windows Server 2022

```
C:\> pnputil -i -a PROXGB\Winx64\WS2022\vxS.inf
```

- Windows Server 2019

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
```

- Windows Server 2016

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
```

- Windows Server 2012 R2

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

- Windows Server 2012

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

5. Depuis votre ordinateur local, activez l'attribut de mise en réseau améliorée à l'aide de l'une des commandes suivantes:

AWS CLI

[modify-instance-attribute](#) (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support simple
```

PowerShell

[Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

- (Facultatif) Créez une AMI à partir de l'instance, comme décrit dans [Création d'une AMI basée sur Amazon EBS](#). L'AMI hérite de l'attribut de mise en réseau améliorée de l'instance. Par conséquent, vous pouvez utiliser cet AMI pour lancer une autre instance avec la mise en réseau améliorée activée par défaut.
- Depuis votre ordinateur local, démarrez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [start-instances](#) (AWS CLI), [Start-EC2Instance](#) (AWS Tools for Windows PowerShell). Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.

Résoudre les problèmes de connectivité

Si vous perdez la connexion tout en activant la mise en réseau améliorée, il se peut que le module `ixgbevf` ne soit pas compatible avec le noyau. Essayez d'installer la version du module `ixgbevf` fournie avec la distribution de Linux pour votre instance.

Si vous activez la mise en réseau améliorée pour une instance de paravirtualisation ou une AMI, votre instance peut devenir inaccessible.

Pour plus d'informations, consultez [Comment activer et configurer la mise en réseau améliorée sur mes instances EC2 ?](#)

Contrôlez les performances réseau de votre instance EC2

Le pilote Elastic Network Adapter (ENA) publie les métriques de performances réseau à partir des instances où elles sont activées. Vous pouvez utiliser ces métriques pour résoudre les problèmes de

performances d'instance, choisir la taille d'instance appropriée pour une charge de travail, planifier les activités de mise à l'échelle de manière proactive et comparer les applications afin de déterminer si elles optimisent les performances disponibles sur une instance.

Amazon EC2 définit les valeurs maximales du réseau au niveau de l'instance afin de garantir une expérience réseau de haute qualité, notamment des performances réseau cohérentes quelle que soit la taille des instances. AWS fournit les valeurs maximales suivantes pour chaque instance :

- Capacité de bande passante : chaque instance EC2 dispose d'une bande passante maximale pour le trafic entrant et sortant agrégé, en fonction du type et de la taille de l'instance. Certaines instances utilisent un mécanisme de crédit I/O réseau pour attribuer la bande passante réseau en fonction de l'utilisation moyenne de la bande passante. Amazon EC2 dispose également d'une bande passante maximale pour le trafic vers Internet AWS Direct Connect et vers Internet. Pour plus d'informations, consultez [Bande passante réseau d'instance Amazon EC2](#).
- Performances Packet-per-second (PPS) — Chaque instance EC2 possède des performances PPS maximales, en fonction du type et de la taille de l'instance.
- Connexions suivies : le groupe de sécurité assure le suivi de chaque connexion établie pour s'assurer que les paquets de retour sont livrés comme prévu. Il existe un nombre maximal de connexions qui peuvent être suivies par instance. Pour plus d'informations, veuillez consulter [Suivi de connexion de groupe de sécurité](#)
- Accès à un service lien-local : Amazon EC2 fournit un maximum de PPS par interface réseau pour le trafic vers des services tels que le service DNS, le service des métadonnées d'instance et le service Amazon Time Sync.

Lorsque le trafic réseau d'une instance dépasse un maximum, AWS façonne le trafic qui dépasse le maximum en mettant en file d'attente puis en supprimant les paquets réseau. Vous pouvez surveiller lorsque le trafic dépasse un maximum à l'aide des métriques de performances réseau. Ces métriques vous informent en temps réel de l'impact sur le trafic réseau et des éventuels problèmes de performances réseau.

Table des matières

- [Prérequis](#)
- [Métriques du pilote ENA](#)
- [Afficher les métriques de performances réseau de votre instance](#)
- [Métriques pour ENA Express](#)
- [Métriques de performances réseau avec le pilote DPDK pour ENA](#)

- [Métriques sur les instances exécutant FreeBSD](#)

Prérequis

Instances Linux

- Installez le pilote ENA version 2.2.10 ou ultérieure. Pour vérifier la version installée, utilisez la commande `ethtool`. Dans l'exemple suivant, la version répond aux exigences minimales.

```
[ec2-user ~]$ ethtool -i eth0 | grep version
version: 2.2.10
```

Pour mettre à niveau votre pilote ENA, consultez la section [Mise en réseau améliorée](#).

- Pour importer ces métriques sur Amazon CloudWatch, installez l' CloudWatch agent. Pour plus d'informations, consultez la section [Collecter les indicateurs de performance du réseau](#) dans le guide de CloudWatch l'utilisateur Amazon.
- Pour prendre en charge les `conntrack_allowance_available` métriques, installez la version 2.8.1 du pilote ENA.

instances Windows

- Installez le pilote ENA version 2.2.2 ou ultérieure. Pour vérifier la version installée, utilisez le Gestionnaire de périphériques comme suit.
 1. Ouvrez le Gestionnaire de périphériques en exécutant `devmgmt.msc`.
 2. Développez Network Adapters (Cartes réseau).
 3. Sélectionnez Amazon Elastic Network Adapter, puis Propriétés (Propriétés).
 4. Sous l'onglet Driver (Pilote), recherchez Driver Version (Version du pilote).

Pour mettre à niveau votre pilote ENA, consultez la section [Mise en réseau améliorée](#).

- Pour importer ces métriques sur Amazon CloudWatch, installez l' CloudWatch agent. Pour plus d'informations, consultez la section [Collecter des métriques réseau avancées](#) dans le guide de CloudWatch l'utilisateur Amazon.

Métriques du pilote ENA

Le pilote ENA apporte les métriques suivantes à l'instance en temps réel. Ces métriques fournissent le nombre cumulé de paquets mis en file d'attente ou ignorés sur chaque interface réseau depuis la dernière réinitialisation du pilote.

Métrique	Description	Pris en charge sur
<code>bw_in_allowance_exceeded</code>	Nombre de paquets mis en file d'attente ou ignorés flottee que la bande passante agrégée entrante a dépassé le maximum de l'instance.	Tous les types d'instances
<code>bw_out_allowance_exceeded</code>	Nombre de paquets mis en file d'attente ou ignorés flottee que la bande passante agrégée sortante a dépassé le maximum de l'instance.	Tous les types d'instances
<code>contrack_allowance_exceeded</code>	Nombre de paquets ignorés flottee que le suivi des connexions a dépassé le maximum de l'instance et que de nouvelles connexions n'ont pas pu être établies. Cela peut entraîner une perte de paquets pour le trafic vers ou en provenance de l'instance.	Tous les types d'instances
<code>contrack_allowance_available</code>	Nombre de connexions suivies pouvant être établies par l'instance avant d'atteindre l'allocation Connexions suivies de ce type d'instance.	Instances créées uniquement sur le système AWS Nitro
<code>linklocal_allowance_exceeded</code>	Nombre de paquets ignorés abandonné que le PPS du trafic	Tous les types d'instances

Métrique	Description	Pris en charge sur
	vers les services proxy locaux a dépassé le maximum de l'interface réseau. Cela affecte le trafic vers le service DNS, le service des métadonnées d'instance et le service Amazon Time Sync.	
pps_allowance_exceeded	Nombre de paquets mis en file d'attente ou ignorés flotée que le PPS bidirectionnel a dépassé le maximum de l'instance.	Tous les types d'instances

Afficher les métriques de performances réseau de votre instance

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Instances Linux

Vous pouvez publier des métriques dans vos outils favoris pour visualiser les données métriques. Par exemple, vous pouvez publier les statistiques sur Amazon à CloudWatch l'aide de l' CloudWatch agent. L'agent vous permet de sélectionner des métriques individuelles et de contrôler la publication.

Vous pouvez également utiliser la commande `ethtool` pour récupérer les métriques de chaque interface réseau, telles que `eth0`, comme suit.

```
[ec2-user ~]$ ethtool -S eth0
  bw_in_allowance_exceeded: 0
  bw_out_allowance_exceeded: 0
  pps_allowance_exceeded: 0
  conntrack_allowance_exceeded: 0
  linklocal_allowance_exceeded: 0
  conntrack_allowance_available: 136812
```

instances Windows

Vous pouvez afficher les métriques à l'aide de n'importe quel consommateur de compteurs de performances Windows. Les données peuvent être analysées en fonction du `EnaPerfCounters`

manifeste. Il s'agit d'un fichier XML qui définit le fournisseur de compteurs de performances et ses ensembles de compteurs.

Pour installer le manifeste

Si vous avez lancé l'instance à l'aide d'une AMI contenant le pilote ENA 2.2.2 ou version ultérieure, ou si vous avez utilisé le script d'installation dans le package de pilotes pour le pilote ENA 2.2.2, le manifeste est déjà installé. Pour installer le manifeste manuellement, procédez comme suit :

1. Supprimez le manifeste existant à l'aide de la commande suivante :

```
unlodctr /m:EnaPerfCounters.man
```

2. Copiez `EnaPerfCounters.man`, le fichier manifeste, du package d'installation du pilote vers `%SystemRoot%\System32\drivers`.
3. Installez le nouveau manifeste à l'aide de la commande suivante :

```
lodctr /m:EnaPerfCounters.man
```

Pour afficher les métriques à l'aide de Performance Monitor

1. Ouvrez Performance Monitor.
2. Appuyez sur `Ctrl+N` pour ajouter de nouveaux compteurs.
3. Sélectionnez ENA Packets Shaping (Mise en forme de paquets ENA) dans la liste.
4. Sélectionnez les instances à surveiller, puis Add (Ajouter).
5. Choisissez OK.

Métriques pour ENA Express

ENA Express est alimenté par la technologie AWS Scalable Reliable Datagram (SRD). SRD est un protocole de transport réseau à hautes performances qui utilise le routage dynamique pour augmenter le débit et minimiser la latence de queue. Vous pouvez utiliser les métriques ENA Express pour vous assurer que vos instances tirent pleinement parti des améliorations de performances apportées par la technologie SRD, par exemple :

- Évaluez vos ressources pour vous assurer qu'elles disposent d'une capacité suffisante pour établir davantage de connexions SRD.

- Identifiez les problèmes potentiels qui empêchent les paquets sortants éligibles d'utiliser SRD.
- Calculez le pourcentage de trafic sortant qui utilise SRD pour l'instance.
- Calculez le pourcentage de trafic entrant qui utilise SRD pour l'instance.

 Note

Pour produire des métriques, utilisez la version 2.8 ou supérieure du pilote.

Les métriques ENA Express suivantes sont disponibles à l'aide de la commande `ethtool` pour les instances basées sur Linux.

- `ena_srd_mode` : décrit les fonctionnalités ENA Express qui sont activées. Les valeurs sont les suivantes :
 - 0 = ENA Express désactivé, UDP désactivé
 - 1 = ENA Express activé, UDP désactivé
 - 2 = ENA Express désactivé, UDP activé

 Note

Cela se produit uniquement lorsque ENA Express a été initialement activé et que UDP a été configuré pour l'utiliser. La valeur précédente est conservée pour le trafic UDP.

- 3 = ENA Express activé, UDP activé
- `ena_srd_eligible_tx_pkts` : le nombre de paquets réseau envoyés au cours d'une période donnée qui répondent aux exigences SRD en matière d'éligibilité, comme suit :
 - Les types d'instance d'envoi et de réception sont pris en charge. Consultez la table [Types d'instance pris en charge pour ENA Express](#) pour plus d'informations.
 - ENA Express doit être configuré pour les instances d'envoi et de réception.
 - Les instances d'envoi et de réception doivent s'exécuter dans la même zone de disponibilité.
 - Le chemin réseau entre les instances ne doit pas inclure de boîtiers intergiciels. ENA Express ne prend actuellement pas en charge les boîtiers intergiciels.

Note

La métrique d'éligibilité ENA Express couvre les exigences en matière de source et de destination, ainsi que le réseau entre les deux points de terminaison. Les paquets éligibles peuvent toujours être disqualifiés une fois qu'ils ont déjà été comptés. Par exemple, si un paquet éligible dépasse la limite d'unité de transmission maximale (MTU), il revient à une transmission ENA standard, bien que le paquet soit toujours considéré comme éligible dans le compteur.

- `ena_srd_tx_pkts` : nombre de paquets SRD transmis au cours d'une période donnée.
- `ena_srd_rx_pkts` : nombre de paquets SRD reçus au cours d'une période donnée.
- `ena_srd_resource_utilization` : pourcentage de l'utilisation maximale de la mémoire autorisée pour les connexions SRD simultanées que l'instance a consommées.

Pour consulter la liste des mesures filtrées pour ENA Express, exécutez la commande `ethtool` suivante pour votre interface réseau (présentée ici en tant que `eth0`) :

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
  ena_srd_mode: 0
  ena_srd_tx_pkts: 0
  ena_srd_eligible_tx_pkts: 0
  ena_srd_rx_pkts: 0
  ena_srd_resource_utilization: 0
```

Trafic sortant (paquets sortants)

Pour vous assurer que votre trafic sortant utilise SRD comme prévu, comparez le nombre de paquets SRD éligibles (`ena_srd_eligible_tx_pkts`) au nombre de paquets SRD envoyés (`ena_srd_tx_pkts`) sur une période donnée.

Les différences importantes entre le nombre de paquets éligibles et le nombre de paquets SRD envoyés sont souvent dues à des problèmes d'utilisation des ressources. Lorsque la carte réseau attachée à l'instance a épuisé ses ressources maximales, ou si les paquets dépassent la limite MTU, les paquets éligibles ne peuvent pas être transmis via SRD et doivent revenir à la transmission ENA standard. Les paquets peuvent également tomber dans cette lacune lors de migrations en direct ou

de mises à jour de serveurs en direct. Un dépannage supplémentaire est nécessaire pour déterminer la cause racine.

Note

Vous pouvez ignorer les différences mineures occasionnelles entre le nombre de paquets éligibles et le nombre de paquets SRD. Cela peut se produire lorsque votre instance établit une connexion à une autre instance pour le trafic SRD, par exemple.

Pour savoir quel pourcentage de votre trafic sortant total utilise SRD sur une période donnée, comparez le nombre de paquets SRD envoyés (`ena_srd_tx_pkts`) au nombre total de paquets envoyés pour l'instance (`NetworkPacketOut`) pendant cette période.

Trafic entrant (paquets entrants)

Pour savoir quel pourcentage de votre trafic entrant utilise le SRD, comparez le nombre de paquets SRD reçus (`ena_srd_rx_pkts`) sur une période donnée au nombre total de paquets reçus pour l'instance (`NetworkPacketIn`) pendant cette période.

Utilisation des ressources

L'utilisation des ressources est basée sur le nombre de connexions SRD simultanées qu'une seule instance peut détenir à un moment donné. La métrique d'utilisation des ressources (`ena_srd_resource_utilization`) assure le suivi de votre utilisation actuelle pour l'instance. À mesure que l'utilisation approche les 100 %, vous pouvez vous attendre à des problèmes de performances. ENA Express passe de la transmission SRD à la transmission ENA standard, et le risque de perte de paquets augmente. Une utilisation élevée des ressources indique qu'il est temps de réduire la taille de l'instance afin d'améliorer les performances réseau.

Note

Lorsque le trafic réseau d'une instance dépasse un maximum, AWS façonne le trafic qui dépasse le maximum en mettant en file d'attente puis en supprimant les paquets réseau.

Persistance

Les métriques de sortie et d'entrée s'accumulent lorsque ENA Express est activé pour l'instance. Les métriques cessent de s'accumuler si ENA Express est désactivé, mais elles persistent tant que

l'instance est toujours en cours d'exécution. Les métriques sont réinitialisées si l'instance redémarre ou est arrêtée, ou si l'interface réseau est détachée de l'instance.

Métriques de performances réseau avec le pilote DPDK pour ENA

Le pilote ENA version 2.2.0 et versions ultérieures prend en charge la génération de rapports de métriques réseau. DPDK version 20.11 inclut le pilote ENA 2.2.0 et est la première version DPDK à prendre en charge cette fonction.

Vous pouvez utiliser un exemple d'application pour afficher les statistiques DPDK. Pour démarrer une version interactive de l'exemple d'application, exécutez la commande suivante.

```
./app/dpdk-testpmd -- -i
```

Dans cette session interactive, vous pouvez saisir une commande afin de récupérer des statistiques étendues pour un port. L'exemple de commande suivant récupère les statistiques pour le port 0.

```
show port xstats 0
```

Voici un exemple de séance interactive avec l'exemple d'application DPDK.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
EAL: Detected 4 lcore(s)
EAL: Detected 1 NUMA nodes
EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
EAL: Selected IOVA mode 'PA'
EAL: Probing VFIO support...
EAL: Invalid NUMA socket, default to 0
EAL: Invalid NUMA socket, default to 0
EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
EAL: No legacy callbacks, legacy socket not created
Interactive-mode selected

Port 0: link state change event
testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
testpmd: preferred mempool ops selected: ring_mp_mc

Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.
```

```
Configuring Port 0 (socket 0)
Port 0: 02:C7:17:A2:60:B1
Checking link statuses...
Done
Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
testpmd> show port xstats 0
##### NIC extended statistics for port 0
rx_good_packets: 0
tx_good_packets: 0
rx_good_bytes: 0
tx_good_bytes: 0
rx_missed_errors: 0
rx_errors: 0
tx_errors: 0
rx_mbuf_allocation_errors: 0
rx_q0_packets: 0
rx_q0_bytes: 0
rx_q0_errors: 0
tx_q0_packets: 0
tx_q0_bytes: 0
wd_expired: 0
dev_start: 1
dev_stop: 0
tx_drops: 0
bw_in_allowance_exceeded: 0
bw_out_allowance_exceeded: 0
pps_allowance_exceeded: 0
contrack_allowance_exceeded: 0
linklocal_allowance_exceeded: 0
rx_q0_cnt: 0
rx_q0_bytes: 0
rx_q0_refill_partial: 0
rx_q0_bad_csum: 0
rx_q0_mbuf_alloc_fail: 0
rx_q0_bad_desc_num: 0
rx_q0_bad_req_id: 0
tx_q0_cnt: 0
tx_q0_bytes: 0
tx_q0_prepare_ctx_err: 0
tx_q0_linearize: 0
tx_q0_linearize_failed: 0
tx_q0_tx_poll: 0
tx_q0_doorbells: 0
```

```
tx_q0_bad_req_id: 0
tx_q0_available_desc: 1023
testpmd>
```

Pour en savoir plus sur l'exemple d'application et son utilisation pour récupérer des statistiques étendues, consultez la section [Testpmd Application User Guide](#) de la documentation DPDK.

Métriques sur les instances exécutant FreeBSD

À partir de la version 2.3.0, le pilote ENA FreeBSD prend en charge la collecte des métriques de performance réseau sur les instances exécutant FreeBSD. Pour activer la collecte des métriques FreeBSD, saisissez la commande suivante et définissez *interval* (l'intervalle) sur une valeur comprise entre 1 et 3 600. Cette valeur spécifie la fréquence, en secondes, à laquelle les métriques FreeBSD sont collectées.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Par exemple, la commande suivante définit la collecte des métriques FreeBSD par le pilote sur l'interface réseau une fois toutes les 10 secondes :

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Pour désactiver la collecte des métriques FreeBSD, vous pouvez exécuter la même commande et définir l'*intervalle* sur 0.

Après avoir activé la collecte des métriques FreeBSD, vous pouvez récupérer le dernier ensemble de métriques collectées en exécutant la commande suivante.

```
sysctl dev.ena.network_interface.eni_metrics
```

Résoudre les problèmes liés à l'adaptateur réseau Elastic sous Linux

Elastic Network Adapter (ENA) est conçu pour améliorer l'intégrité du système d'exploitation et réduire les risques de perturbations à long terme en raison d'un comportement inattendu de matériel ou de défaillances. L'architecture ENA assure une transparence optimale des défaillances de périphériques ou de pilotes auprès du système. Cette rubrique fournit des informations de dépannage pour ENA.

Si vous ne pouvez pas vous connecter à votre instance, commencez par la section [Résoudre les problèmes de connectivité](#).

Si vous constatez une dégradation des performances après la migration vers un type d'instance de sixième génération, consultez l'article [Que dois-je faire avant de migrer mon instance EC2 vers une instance de sixième génération afin de garantir des performances réseau optimales ?](#)

Si vous ne parvenez pas à vous connecter à votre instance, recueillez des informations de diagnostic à l'aide des mécanismes de détection des défaillances et de récupération couverts dans des sections ultérieures de cette rubrique.

Sommaire

- [Résoudre les problèmes de connectivité](#)
- [Mécanisme Keep-alive](#)
- [Expiration du délai d'attente des opérations de lecture](#)
- [Statistiques](#)
- [Journaux d'erreur de pilote dans syslog](#)
- [Notifications de configuration sous-optimales](#)

Résoudre les problèmes de connectivité

Si vous perdez la connexion lors de l'activation de la mise en réseau améliorée, il se peut que le module ena ne soit pas compatible avec le noyau de votre instance. Cela peut se produire si vous installez le module pour une version de noyau spécifique (sans dkms ou avec un fichier dkms.conf mal configuré), puis que le noyau de votre instance est mis à jour. Si le module ena du noyau de l'instance qui est chargé au moment du démarrage n'est pas correctement installé, votre instance ne reconnaît pas la carte réseau et devient inaccessible.

Si vous activez la mise en réseau améliorée pour une instance de paravirtualisation (PV) ou une AMI, votre instance peut devenir inaccessible.

Si votre instance devient inaccessible après l'activation de la mise en réseau améliorée via ENA, vous pouvez désactiver l'attribut `enaSupport` pour votre instance afin qu'elle utilise une autre carte réseau à la place.

Pour désactiver la mise en réseau améliorée via ENA (instances basées sur EBS)

1. Depuis votre ordinateur local, arrêtez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [stop-instances](#) (AWS CLI), (`stop-ec2-instance`). [Stop-EC2Instance](#) AWS Tools for Windows PowerShell Si votre instance est gérée par AWS OpsWorks, vous devez l'arrêter dans la AWS OpsWorks console afin que son état reste synchronisé.

⚠ Important

Si vous utilisez une instance basée sur le stockage d'instance, vous ne pouvez pas l'arrêter. A la place, passez à [Pour désactiver la mise en réseau améliorée via ENA \(instances basées sur le stockage d'instance\)](#).

2. Depuis votre ordinateur local, désactivez l'attribut de mise en réseau améliorée à l'aide de la commande suivante.

- [modify-instance-attribute](#) (AWS CLI)

```
$ C:\> aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
```

3. Depuis votre ordinateur local, démarrez l'instance à l'aide de la console Amazon EC2 ou de l'une des commandes suivantes : [start-instances](#) (AWS CLI), [Start-EC2Instance\(\)](#). AWS Tools for Windows PowerShell Si votre instance est gérée par AWS OpsWorks, vous devez démarrer l'instance dans la AWS OpsWorks console afin que son état reste synchronisé.
4. (Facultatif) Connectez-vous à votre instance et essayez de réinstaller le module ena avec votre version de noyau actuelle en suivant les étapes décrites dans la section [Activez une mise en réseau améliorée avec l'Elastic Network Adapter \(ENA\) sur vos instances EC2](#).

Pour désactiver la mise en réseau améliorée via ENA (instances basées sur le stockage d'instance)

Si votre instance est basée sur le stockage d'instance, créez une AMI, comme décrit dans la section [Créer une AMI Linux basée sur le stockage d'instance](#). Veillez à désactiver l'attribut `enaSupport` de mise en réseau améliorée lorsque vous inscrivez l'AMI.

- [register-image](#) (AWS CLI)

```
$ C:\> aws ec2 register-image --no-ena-support ...
```

- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
C:\> Register-EC2Image -EnaSupport $false ...
```

Mécanisme Keep-alive

Le dispositif ENA publie des événements keep-alive selon une fréquence fixe (généralement une fois par seconde). Le pilote ENA implémente un mécanisme de surveillance, qui recherche la présence de ces messages keep-alive. Si un ou plusieurs messages sont présents, la surveillance est réarmée. Dans le cas contraire, le pilote conclut que l'appareil a subi une défaillance et effectue alors les opérations suivantes :

- Il envoie ses statistiques dans le journal système.
- Il réinitialise le dispositif ENA.
- Il réinitialise l'état du pilote ENA.

La procédure de réinitialisation ci-dessus peut entraîner une perte de trafic pour une courte période de temps (la récupération des connexions TCP doit être possible), mais ne devrait pas affecter l'utilisateur.

Le dispositif ENA peut également demander indirectement une procédure de réinitialisation de l'appareil. Dans ce cas, il n'envoie pas de notification keep-alive. Cela est possible, par exemple, si le périphérique ENA atteint un état inconnu après le chargement d'une configuration irrécupérable.

Voici un exemple de procédure de réinitialisation :

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.....
.....
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
end of the down process, the driver discards incomplete packets.
```

```
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
[Wed Apr 6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
process is complete
```

Expiration du délai d'attente des opérations de lecture

L'architecture ENA propose une utilisation limitée des opérations de lecture des I/O mappées par la mémoire (MMIO). Le pilote du périphérique ENA n'accède aux registres MMIO que lors de la procédure d'initialisation.

Si les journaux du pilote (disponibles dans la sortie `dmesg`) indiquent une défaillance des opérations de lecture, un pilote incompatible ou mal compilé, un dispositif saturé ou une défaillance matérielle peuvent en être la cause.

Les entrées de journal intermittentes qui indiquent des défaillances des opérations de lecture ne sont pas problématiques. Dans ce cas, le pilote réessaie de les traiter. Toutefois, une série d'entrées de journal contenant des défaillances de lecture indique un problème de pilote ou de matériel.

Voici un exemple d'entrée de journal pilote indiquant une défaillance des opérations de lecture en raison de l'expiration d'un délai d'attente :

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
expected: req id[2] offset[8] actual: req id[57007] offset[0]
```

```
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistiques

Si vous rencontrez des problèmes de latence ou si les performances réseau sont insuffisantes, vous devez récupérer les statistiques de l'appareil et les examiner. Pour obtenir ces statistiques, utilisez `ethtool`, comme suit.

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
tx_timeout: 0
suspend: 0
resume: 0
wd_expired: 0
interface_up: 1
interface_down: 0
admin_q_pause: 0
bw_in_allowance_exceeded: 0
bw_out_allowance_exceeded: 0
pps_allowance_exceeded: 0
contrack_allowance_available: 450878
contrack_allowance_exceeded: 0
linklocal_allowance_exceeded: 0
queue_0_tx_cnt: 4329
queue_0_tx_bytes: 1075749
queue_0_tx_queue_stop: 0
...
```

Les paramètres de sortie de commande suivants sont décrits ci-dessous :

`tx_timeout: N`

Nombre de fois que la surveillance Netdev a été activée.

`suspend: N`

Nombre de fois que le pilote a effectué une opération de suspension.

`resume: N`

Nombre de fois que le pilote a effectué une opération de reprise.

`wd_expired`: *N*

Nombre de fois que le pilote n'a pas reçu l'événement keep-alive au cours des trois secondes précédentes.

`interface_up`: *N*

Nombre de fois que l'interface ENA a été affichée.

`interface_down`: *N*

Nombre de fois que l'interface ENA a été fermée.

`admin_q_pause`: *N*

Nombre de fois que la file d'attente d'administration n'a pas été trouvée dans un état en cours d'exécution.

`bw_in_allowance_exceeded`: *N*

Nombre de paquets mis en file d'attente ou ignorés flottee que la bande passante agrégée entrante a dépassé le maximum de l'instance.

`bw_out_allowance_exceeded`: *N*

Nombre de paquets mis en file d'attente ou ignorés flottee que la bande passante agrégée sortante a dépassé le maximum de l'instance.

`pps_allowance_exceeded`: *N*

Nombre de paquets mis en file d'attente ou ignorés flottee que le PPS bidirectionnel a dépassé le maximum de l'instance.

`contrack_allowance_available`: *N*

Nombre de connexions suivies pouvant être établies par l'instance avant d'atteindre l'allocation Connexions suivies de ce type d'instance. Disponible uniquement pour les instances basées sur Nitro. Non compatible avec les instances FreeBSD ou les environnements DPDK.

`contrack_allowance_exceeded`: *N*

Nombre de paquets ignorés flottee que le suivi des connexions a dépassé le maximum de l'instance et que de nouvelles connexions n'ont pas pu être établies. Cela peut entraîner une perte de paquets pour le trafic vers ou en provenance de l'instance.

`linklocal_allowance_exceeded`: *N*

Nombre de paquets ignorés abandonné que le PPS du trafic vers les services proxy locaux a dépassé le maximum de l'interface réseau. Cela affecte le trafic vers le service DNS, le service des métadonnées d'instance et le service Amazon Time Sync.

`queue_N_tx_cnt`: *N*

Nombre de paquets transmis pour cette file d'attente.

`queue_N_tx_bytes`: *N*

Nombre d'octets transmis pour cette file d'attente.

`queue_N_tx_queue_stop`: *N*

Nombre de fois que la file d'attente *N* était pleine et qu'elle a été arrêtée.

`queue_N_tx_queue_wakeup`: *N*

Nombre de fois que la file d'attente *N* a repris après avoir été arrêtée.

`queue_N_tx_dma_mapping_err`: *N*

Nombre d'erreurs d'accès direct à la mémoire. Si cette valeur ne correspond pas à 0, les ressources système sont faibles.

`queue_N_tx_linearize`: *N*

Nombre de fois que la linéarisation SKB a été tentée pour cette file d'attente.

`queue_N_tx_linearize_failed`: *N*

Nombre de fois que la linéarisation SKB a échoué pour cette file d'attente.

`queue_N_tx_napi_comp`: *N*

Nombre de fois que le gestionnaire `napi` a appelé `napi_complete` pour cette file d'attente.

`queue_N_tx_tx_poll`: *N*

Nombre de fois que le gestionnaire `napi` a été planifié pour cette file d'attente.

`queue_N_tx_doorbells`: *N*

Nombre de portes de transmission pour cette file d'attente.

`queue_N_tx_prepare_ctx_err: N`

Nombre de fois que `ena_com_prepare_tx` a échoué pour cette file d'attente.

`queue_N_tx_bad_req_id: N`

`req_id` non valide pour cette file d'attente. La valeur `req_id` valide est égale à zéro, moins la valeur `queue_size`, moins 1.

`queue_N_tx_llq_buffer_copy: N`

Nombre de paquets dont la taille des en-têtes est supérieure à l'entrée `llq` pour cette file d'attente.

`queue_N_tx_missed_tx: N`

Nombre de paquets qui n'ont pas été traités entièrement pour cette file d'attente.

`queue_N_tx_unmask_interrupt: N`

Nombre de fois que `tx interrupt` a été démasqué pour cette file d'attente.

`queue_N_rx_cnt: N`

Nombre de paquets reçus pour cette file d'attente.

`queue_N_rx_bytes: N`

Nombre d'octets reçus pour cette file d'attente.

`queue_N_rx_rx_copybreak_pkt: N`

Nombre de fois que la file d'attente `rx` a reçu un paquet inférieur à la taille de paquet `rx_copybreak` pour cette file d'attente.

`queue_N_rx_csum_good: N`

Nombre de fois que la file d'attente `rx` a reçu un paquet dont le total de contrôle a été vérifié comme étant correct pour cette file d'attente.

`queue_N_rx_refil_partial: N`

Nombre de fois que le pilote n'a pas réussi à remplir la portion vide de la file d'attente `rx` avec les tampons pour cette file d'attente. Si cette valeur n'est pas égale à zéro, les ressources mémoire sont faibles.

`queue_N_rx_bad_csum: N`

Nombre de fois que la file d'attente `rx` a reçu un mauvais total de contrôle pour cette file d'attente (uniquement si le déchargement du total de contrôle `rx` est pris en charge).

queue_#_rx_page_alloc_fail: *N*

Nombre de fois que l'allocation des pages a échoué pour cette file d'attente. Si cette valeur n'est pas égale à zéro, les ressources mémoire sont faibles.

queue_#_rx_skb_alloc_fail: *N*

Nombre de fois que l'allocation SKB a échoué pour cette file d'attente. Si cette valeur n'est pas égale à zéro, les ressources système sont faibles.

queue_#_rx_dma_mapping_err: *N*

Nombre d'erreurs d'accès direct à la mémoire. Si cette valeur ne correspond pas à 0, les ressources système sont faibles.

queue_#_rx_bad_desc_num: *N*

Trop de tampons par paquet. Si cette valeur n'est pas égale à 0, cela indique l'utilisation de très petits tampons.

queue_#_rx_bad_req_id: *N*

Le req_id de cette file d'attente n'est pas valide. Le req_id valide est de [0, queue_size - 1].

queue_#_rx_empty_rx_ring: *N*

Nombre de fois que la file d'attente rx était vide pour cette file d'attente.

queue_#_rx_csum_unchecked: *N*

Nombre de fois que la file d'attente rx a reçu un paquet dont le total de contrôle n'a pas été vérifié pour cette file d'attente.

queue_#_rx_xdp_aborted: *N*

Nombre de fois qu'un paquet XDP a été classé comme XDP_ABORT.

queue_#_rx_xdp_drop: *N*

Nombre de fois qu'un paquet XDP a été classé comme XDP_DROP.

queue_#_rx_xdp_pass: *N*

Nombre de fois qu'un paquet XDP a été classé comme XDP_PASS.

queue_#_rx_xdp_tx: *N*

Nombre de fois qu'un paquet XDP a été classé comme XDP_TX.

`queue_N_rx_xdp_invalid: N`

Nombre de fois que le code de retour XDP du paquet n'était pas valide.

`queue_N_rx_xdp_redirect: N`

Nombre de fois qu'un paquet XDP a été classé comme XDP_REDIRECT.

`queue_N_xdp_tx_cnt: N`

Nombre de paquets transmis pour cette file d'attente.

`queue_N_xdp_tx_bytes: N`

Nombre d'octets transmis pour cette file d'attente.

`queue_N_xdp_tx_queue_stop: N`

Nombre de fois que cette file d'attente était pleine et qu'elle a été arrêtée.

`queue_N_xdp_tx_queue_wakeup: N`

Nombre de fois que cette file d'attente a repris après avoir été arrêtée.

`queue_N_xdp_tx_dma_mapping_err: N`

Nombre d'erreurs d'accès direct à la mémoire. Si cette valeur ne correspond pas à 0, les ressources système sont faibles.

`queue_N_xdp_tx_linearize: N`

Nombre de fois que la linéarisation du tampon XDP a été tentée pour cette file d'attente.

`queue_N_xdp_tx_linearize_failed: N`

Nombre de fois que la linéarisation du tampon XDP a échoué pour cette file d'attente.

`queue_N_xdp_tx_napi_comp: N`

Nombre de fois que le gestionnaire napi a appelé napi_complete pour cette file d'attente.

`queue_N_xdp_tx_tx_poll: N`

Nombre de fois que le gestionnaire napi a été planifié pour cette file d'attente.

`queue_N_xdp_tx_doorbells: N`

Nombre de portes de transmission pour cette file d'attente.

`queue_N_xdp_tx_prepare_ctx_err: N`

Nombre de fois que `ena_com_prepar_tx` a échoué pour cette file d'attente. Cette valeur doit toujours être égale à zéro. Si ce n'est pas le cas, consultez les journaux du pilote.

`queue_N_xdp_tx_bad_req_id: N`

Le `req_id` de cette file d'attente n'est pas valide. Le `req_id` valide est de `[0, queue_size - 1]`.

`queue_N_xdp_tx_llq_buffer_copy: N`

Nombre de paquets dont les en-têtes ont été copiés à l'aide de la copie tampon llq pour cette file d'attente.

`queue_N_xdp_tx_missed_tx: N`

Nombre de fois qu'une entrée de file d'attente tx a dépassé un délai de résiliation pour cette file d'attente.

`queue_N_xdp_tx_unmask_interrupt: N`

Nombre de fois que tx interrupt a été démasqué pour cette file d'attente.

`ena_admin_q_aborted_cmd: N`

Nombre de commandes d'administration qui ont été abandonnées. Généralement, cela se produit lors de la procédure de récupération automatique.

`ena_admin_q_submitted_cmd: N`

Nombre de portes d'administration de la file d'attente.

`ena_admin_q_completed_cmd: N`

Nombre de finalisations de la file d'attente d'administration.

`ena_admin_q_out_of_space: N`

Nombre de fois que le pilote a essayé de présenter la nouvelle commande d'administration, mais que la file d'attente était pleine.

`ena_admin_q_no_completion: N`

Nombre de fois que l'administration du pilote n'a pas été terminée pour une commande.

Journaux d'erreur de pilote dans syslog

Le pilote ENA écrit les messages journaux dans syslog pendant le démarrage du système. Vous pouvez examiner ces journaux pour rechercher les erreurs si vous rencontrez des problèmes. Voici un exemple d'informations enregistrées par le pilote ENA dans syslog pendant le démarrage du système, ainsi que des annotations pour certains messages.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 478.416939] [ENA_COM:
ena_com_validate_version] ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 478.420915] [ENA_COM:
ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.256831] ena 0000:00:03.0: Device
watchdog is Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.672947] ena 0000:00:03.0: creating 8 io
queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.680885] [ENA_COM:
ena_com_init_interrupt_moderation] Feature 20 isn't supported // Interrupt moderation
is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.691609] [ENA_COM:
ena_com_get_feature_ex] Feature 10 isn't supported // RSS HASH function configuration
is not supported by the
device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.694583] [ENA_COM:
ena_com_get_feature_ex] Feature 18 isn't supported //RSS HASH input source
configuration is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.697433] [ENA_COM:
ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.701064] ena 0000:00:03.0 (unnamed
net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.704917] ena 0000:00:03.0: Elastic
Network Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 480.805037] EXT4-fs (xvda1): re-mounted.
Opts: (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 481.025842] NET: Registered protocol family
10
```

Quelles sont les erreurs que je peux ignorer ?

Les avertissements suivants qui peuvent apparaître dans les journaux d'erreur de votre système peuvent être ignorés pour Elastic Network Adapter :

Set host attribute isn't supported

Les attributs de l'hôte ne sont pas pris en charge pour cet appareil.

failed to alloc buffer for rx queue

Il s'agit d'une erreur récupérable. Elle indique qu'il y a peut-être eu un problème de pression de mémoire lorsque l'erreur a été lancée.

Feature **X** isn't supported

La fonctionnalité référencée n'est pas prise en charge par Elastic Network Adapter. Les valeurs possibles pour **X** incluent :

- **10** : la configuration de la fonction de hachage RSS n'est pas prise en charge pour cet appareil.
- **12** : la configuration de la table d'indirection RSS n'est pas prise en charge pour cet appareil.
- **18** : la configuration des entrées de hachage RSS n'est pas prise en charge pour cet appareil.
- **20** : la modération d'interruption n'est pas prise en charge pour cet appareil.
- **27** : le pilote ENA (Elastic Network Adapter) ne prend pas en charge l'interrogation des fonctions Ethernet à partir de snmpd.

Failed to config AENQ

Elastic Network Adapter ne prend pas en charge la configuration AENQ.

Trying to set unsupported AENQ events

Cette erreur indique une tentative de définition d'un groupe d'événements AENQ qui n'est pas pris en charge par Elastic Network Adapter.

Notifications de configuration sous-optimales

Le dispositif ENA détecte les paramètres de configuration sous-optimaux dans le pilote que vous pouvez modifier. Le périphérique avertit le pilote ENA et journalise un avertissement sur la console. L'exemple suivant montre le format du message d'avertissement.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for additional details and mitigation options.
```

La liste suivante indique les détails du code de notification et les actions recommandées pour les résultats de configuration sous-optimaux.

- Code **1** : ENA Express avec une configuration LLQ étendue n'est pas recommandé

L'ENI ENA Express est configuré avec un LLQ étendu. Cette configuration n'est pas optimale et pourrait avoir un impact sur les performances d'ENA Express. Nous vous recommandons de désactiver les paramètres LLQ étendus lorsque vous utilisez les ENI ENA Express comme suit.

```
sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
```

Pour en savoir plus sur la syntaxe des expressions pour ENA Express, consultez [Améliorez les performances du réseau avec ENA Express sur vos instances EC2](#).

- Code 2 : ENA Express ENI avec une profondeur de file d'attente Tx non optimale n'est pas recommandé

L'ENI ENA Express est configuré avec une profondeur de file d'attente Tx non optimale. Cette configuration pourrait avoir un impact sur les performances d'ENA Express. Nous vous recommandons d'agrandir toutes les files d'attente Tx à la valeur maximale de l'interface réseau lorsque vous utilisez les ENI ENA Express comme suit.

Vous pouvez exécuter les `ethtool` commandes suivantes pour ajuster la taille du LLQ. Pour en savoir plus sur la façon de contrôler, d'interroger et d'activer Wide-LLQ, consultez la rubrique [Large Low-Latency Queue \(Large LLQ\)](#) de la documentation relative au pilote de noyau Linux pour ENA dans le référentiel Amazon Drivers. GitHub

```
ethtool -g interface
```

Réglez vos files d'attente Tx à la profondeur maximale :

```
ethtool -G interface tx depth
```

Pour en savoir plus sur la syntaxe des expressions pour ENA Express, consultez [Améliorez les performances du réseau avec ENA Express sur vos instances EC2](#).

- Code 3 : ENA avec une taille LLQ normale et le trafic de paquets Tx dépasse la taille maximale d'en-tête prise en charge

Par défaut, ENA LLQ prend en charge la taille d'en-tête de paquet Tx jusqu'à 96 octets. Si la taille de l'en-tête du paquet est supérieure à 96 octets, le paquet est supprimé. Pour atténuer ce problème, nous vous recommandons d'activer Wide-LLQ, qui augmente la taille d'en-tête de paquet Tx prise en charge à un maximum de 224 octets.

Toutefois, lorsque vous activez Wide-LLQ, la taille maximale de l'anneau Tx est réduite de 1 000 à 512 entrées. Wide-LLQ est activé par défaut pour tous les types d'instances de Nitro v4 et versions ultérieures.

- Les types d'instances Nitro v4 ont une taille d'anneau Wide-LLQ Tx maximale par défaut de 512 entrées, qui ne peut pas être modifiée.
- Les types d'instances Nitro v5 ont une taille d'anneau Wide-LLQ Tx par défaut de 512 entrées, que vous pouvez augmenter jusqu'à 1 000 entrées.

Vous pouvez exécuter les `ethtool` commandes suivantes pour ajuster la taille du LLQ. Pour en savoir plus sur la façon de contrôler, d'interroger et d'activer Wide-LLQ, consultez la rubrique [Large Low-Latency Queue \(Large LLQ\)](#) de la documentation relative au pilote de noyau Linux pour ENA dans le référentiel Amazon Drivers. GitHub

Trouvez la profondeur maximale de vos files d'attente Tx :

```
ethtool -g interface
```

Réglez vos files d'attente Tx à la profondeur maximale :

```
ethtool -G interface tx depth
```

Résoudre les problèmes liés au pilote Windows d'Elastic Network Adapter

Elastic Network Adapter (ENA) est conçu pour améliorer l'état du système d'exploitation et réduire les comportements ou les échecs inattendus qui peuvent perturber les opérations de votre instance Windows. L'architecture ENA assure une transparence optimale des défaillances de périphériques ou de pilotes auprès du système d'exploitation.

Installation du pilote Elastic Network Adapter (ENA)

Si votre instance n'est pas basée sur l'une des dernières Amazon Machine Image (AMI) Windows fournies par Amazon, utilisez la procédure suivante pour installer le pilote ENA actuel sur votre instance. Vous devez effectuer cette mise à jour à un moment où il est possible de redémarrer votre instance. Si le script d'installation ne redémarre pas automatiquement votre instance, nous vous recommandons de redémarrer l'instance à la dernière étape.

Si vous utilisez un volume de stockage d'instances pour stocker des données pendant que l'instance fonctionne, ces données sont effacées lorsque vous arrêtez l'instance. Avant d'arrêter votre instance, vérifiez que vous avez copié toutes les données dont vous avez besoin à partir de vos volumes de stockage d'instances vers un stockage persistant, tel qu'Amazon EBS ou Amazon S3.

Prérequis

Pour installer ou mettre à niveau le pilote ENA, votre instance Windows doit remplir les conditions préalables suivantes :

- Avoir installé PowerShell la version 3.0 ou ultérieure

Étape 1 : sauvegarder vos données

Nous vous recommandons de créer une AMI de sauvegarde au cas où vous auriez besoin d'annuler vos modifications via le Gestionnaire de périphériques. Pour créer une AMI de sauvegarde avec le AWS Management Console, procédez comme suit :

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance qui nécessite la mise à niveau du pilote, puis choisissez Arrêter l'instance dans le menu État de l'instance.
4. Une fois l'instance arrêtée, sélectionnez-la à nouveau. Pour créer votre sauvegarde, choisissez Image et modèles dans le menu Actions, puis choisissez Créer une image.
5. Pour redémarrer votre instance, choisissez Démarrer l'instance dans le menu État de l'instance.

Étape 2 : installer ou mettre à niveau votre pilote ENA

Vous pouvez installer ou mettre à niveau votre pilote ENA avec le AWS Systems Manager distributeur ou avec des PowerShell applets de commande. Pour plus d'instructions, sélectionnez l'onglet correspondant à la méthode que vous voulez utiliser.

Systems Manager Distributor

Vous pouvez utiliser la fonctionnalité Systems Manager Distributor pour déployer des packages sur vos nœuds gérés par Systems Manager. Avec Systems Manager Distributor, vous pouvez installer le package du pilote ENA une seule fois ou avec des mises à jour planifiées. Pour plus d'informations sur l'installation du package de pilotes ENA (`AwsEnaNetworkDriver`) avec

Systems Manager Distributor, consultez [Installation ou mise à jour des packages](#) dans le Guide de l'utilisateur AWS Systems Manager .

PowerShell

Cette section explique comment télécharger et installer des packages de pilotes ENA sur votre instance à l'aide de PowerShell applets de commande.

Option 1 : télécharger et extraire la dernière version

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Utilisez la cmdlet `invoke-webrequest` pour télécharger le dernier package de pilotes :

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

Note

Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, il est possible que le protocole TLS 1.2 doive être activé sur votre PowerShell terminal. Vous pouvez activer le protocole TLS 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
```

Vous pouvez également télécharger le package de pilotes le plus récent à partir d'une fenêtre de navigateur sur votre instance.

3. Utilisez la cmdlet `expand-archive` pour extraire l'archive zip que vous avez téléchargée sur votre instance :

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Option 2 : télécharger et extraire une version spécifique

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Téléchargez le package de pilotes ENA correspondant à la version spécifique que vous voulez à partir du lien de version dans le tableau [pilote Windows ENA](#).
3. Décompressez l'archive zip dans votre instance.

Installez le pilote ENA avec PowerShell

Les étapes d'installation sont les mêmes, que vous ayez téléchargé le dernier pilote ou une version spécifique. Pour installer le pilote ENA, procédez comme suit.

1. Pour installer le pilote, exécutez le `install.ps1` PowerShell script depuis le `AwsEnaNetworkDriver` répertoire de votre instance. Si un message d'erreur s'affiche, assurez-vous que vous utilisez la PowerShell version 3.0 ou une version ultérieure.
2. Si le programme d'installation ne redémarre pas automatiquement votre instance, exécutez l'`Restart-Computer` PowerShell applet de commande.

```
PS C:\> Restart-Computer
```

Étape 3 (facultative) : vérifier la version du pilote ENA après l'installation

Pour vous assurer que le package du pilote ENA a été installé avec succès sur votre instance, vous pouvez vérifier la nouvelle version comme suit :

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.

Note

Les adaptateurs ENA utilisent tous le même pilote. Si vous avez plusieurs adaptateurs ENA, vous pouvez sélectionner n'importe lequel d'entre eux pour mettre à jour le pilote de tous les adaptateurs ENA.

6. Pour vérifier la version actuelle installée, ouvrez l'onglet Pilote et vérifiez la version du pilote. Si la version actuelle ne correspond pas à votre version cible, consultez [Résoudre les problèmes liés au pilote Windows d'Elastic Network Adapter](#).

Annulation de l'installation d'un pilote ENA

En cas de problème lors de l'installation, vous devrez peut-être restaurer le pilote. Suivez ces étapes pour revenir à la version précédente du pilote ENA qui était installé sur votre instance.

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.

Note

Les adaptateurs ENA utilisent tous le même pilote. Si vous avez plusieurs adaptateurs ENA, vous pouvez sélectionner n'importe lequel d'entre eux pour mettre à jour le pilote de tous les adaptateurs ENA.

6. Pour annuler le pilote, ouvrez l'onglet Pilote et choisissez Annuler le pilote. Cela ouvre la fenêtre Restauration du package de pilotes.

Note

Si l'onglet Pilote n'affiche pas l'action Annuler le pilote, ou si l'action n'est pas disponible, cela signifie que le [magasin de pilotes](#) de votre instance ne contient pas le package de pilotes précédemment installé. Pour résoudre ce problème, consultez [Scénarios de résolution des problèmes](#), et développez la section Version inattendue du pilote ENA installé. Pour plus d'informations sur le processus de sélection du package de pilotes de périphériques, consultez [Comment Windows sélectionne un package de pilotes pour un périphérique](#) sur le site Web de documentation de Microsoft.

Collecter des informations de diagnostic sur l'instance

Les étapes pour ouvrir les outils du système d'exploitation Windows varient en fonction de la version du système d'exploitation installée sur votre instance. Dans les sections suivantes, nous utilisons la boîte de dialogue Exécuter pour ouvrir les outils. Celle-ci fonctionne de la même manière sur toutes les versions du système d'exploitation. Toutefois, vous pouvez accéder à ces outils en suivant n'importe quelle méthode de votre choix.

Accéder à la boîte de dialogue Exécuter

- À l'aide de la combinaison de touches avec le logo Windows : Windows + R
- À l'aide de la barre de recherche :
 - Entrez `run` dans la barre de recherche.
 - Sélectionnez l'application Exécuter à partir des résultats de recherche.

Certaines étapes nécessitent le menu contextuel pour accéder aux propriétés ou aux actions contextuelles. Il existe plusieurs méthodes pour le faire, qui dépendent de la version de système d'exploitation et du matériel dont vous disposez.

Accéder au menu contextuel

- À l'aide de la souris : cliquez avec le bouton droit sur un élément pour afficher son menu contextuel.
- À l'aide de votre clavier :
 - selon la version de votre système d'exploitation, utilisez Shift + F10 ou Ctrl + Shift + F10.

- Si votre clavier contient la touche contextuelle (trois lignes horizontales dans un carré), sélectionnez l'élément souhaité, puis appuyez sur la touche contextuelle.

Si vous pouvez vous connecter à votre instance, utilisez les techniques suivantes pour collecter des informations de diagnostic à des fins de dépannage.

Vérifier l'état du dispositif ENA

Pour vérifier l'état de votre pilote Windows ENA à l'aide du Gestionnaire de périphériques Windows, procédez comme suit :

1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.
2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.
6. Vérifiez que le message de l'onglet Général indique « Ce périphérique fonctionne correctement. »

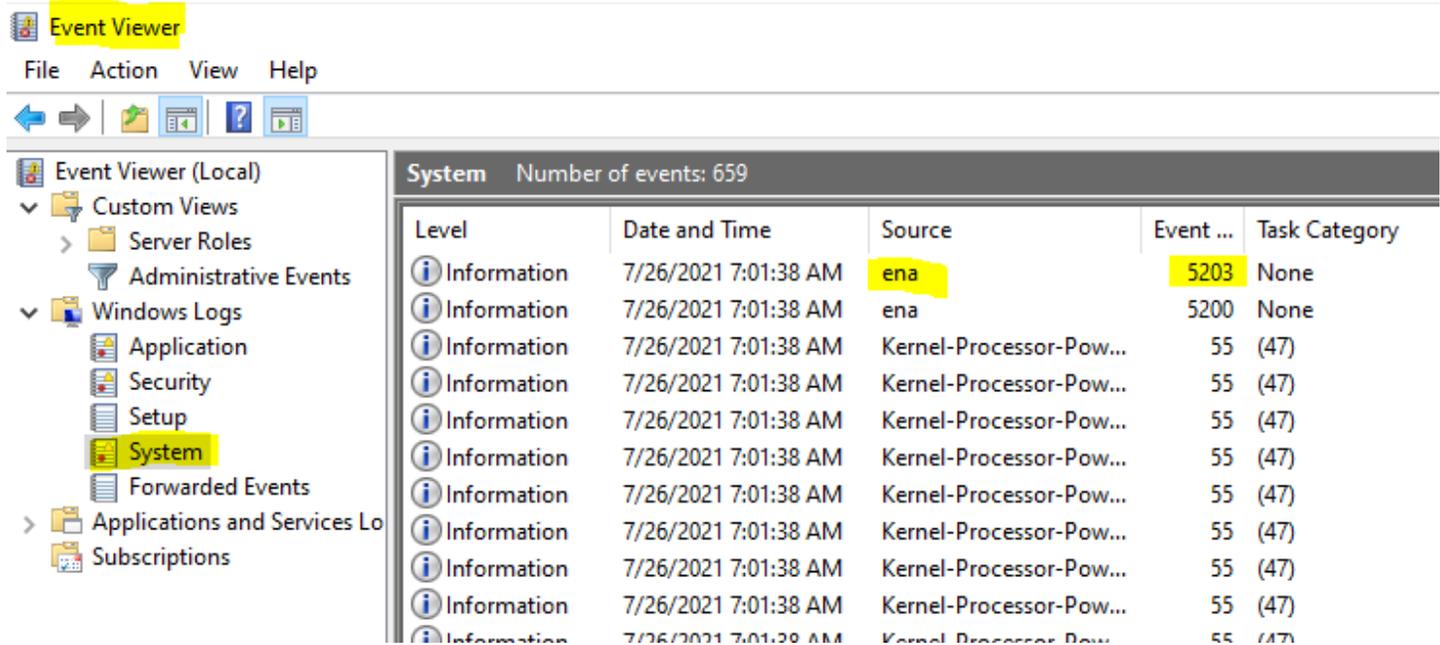
Examiner les messages d'événements du pilote

Pour consulter les journaux d'événements du pilote Windows ENA à l'aide de l'Observateur d'événements Windows, procédez comme suit :

1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.
2. Pour ouvrir l'Observateur d'événements Windows, saisissez `eventvwr.msc` dans la fenêtre Exécuter.
3. Choisissez OK. La fenêtre de l'Observateur d'événements s'ouvre.
4. Développez le menu Journaux Windows, puis choisissez Système.
5. Sous Actions, dans le panneau supérieur droit, choisissez Créer une vue personnalisée. La boîte de dialogue Filtrer s'affiche.
6. Dans la zone Sources d'événements, saisissez `ena`. Cela limite les résultats aux événements générés par le pilote Windows ENA.

7. Choisissez OK. Les résultats du journal d'événements filtrés s'affichent dans les sections des détails de la fenêtre.
8. Pour explorer les détails, sélectionnez un message d'événement dans la liste.

L'exemple suivant montre un événement de pilote ENA dans la liste des événements système de l'Observateur d'événements Windows :



Résumé des messages d'événement

Le tableau suivant présente les messages d'événements générés par le pilote Windows ENA.

Entrée

ID de l'événement	Description de l'événement du pilote ENA	Type
5001	Hardware is out of resources (Le matériel est à court de ressources)	Erreur
5002	Adapter has detected a hardware error (Le dispositif a détecté une erreur matérielle)	Erreur

ID de l'événement	Description de l'événement du pilote ENA	Type
5005	Adapter has timed out on NDIS operation that did not complete in a timely manner (Le dispositif a expiré à l'opération NDIS qui ne s'est pas terminée en temps opportun)	Erreur
5032	Adapter has failed to reset the device (Le dispositif n'a pas réussi à réinitialiser le périphérique)	Erreur
5200	Adapter has been initialized (Le dispositif a été initialisé)	Informationnel
5201	Adapter has been halted (Le dispositif a été interrompu)	Informationnel
5202	Adapter has been paused (Le dispositif a été mis en pause)	Informationnel
5203	Adapter has been restarted (Le dispositif a été redémarré)	Informationnel
5204	Adapter has been shut down (Le dispositif a été arrêté)	Informationnel
5205	Adapter has been reset (Le dispositif a été réinitialisé)	Erreur
5206	Adapter has been surprise removed (Le dispositif a été retiré par surprise)	Erreur

ID de l'événement	Description de l'événement du pilote ENA	Type
5208	Adapter initialization routine has failed (La routine d'initialisation du dispositif a échoué)	Erreur
5210	Adapter has encountered and successfully recovered an internal issue (Le dispositif a rencontré un problème interne et a réussi à récupérer)	Erreur

Vérifier les métriques de performance

Le pilote Windows ENA publie les métriques de performance réseau à partir des métriques où elles sont activées. Vous pouvez afficher et activer les métriques sur l'instance à l'aide de l'application Performance Monitor native. Pour plus d'informations sur les métriques produites par le pilote Windows ENA, consultez [Contrôlez les performances réseau de votre instance EC2](#).

Sur les instances où les métriques ENA sont activées et où l'agent Amazon CloudWatch est installé, il CloudWatch collecte les métriques associées aux compteurs dans Windows Performance Monitor, ainsi que certaines métriques avancées pour l'ENA. Ces métriques sont collectées en plus des métriques activées par défaut sur les instances EC2. Pour plus d'informations sur les statistiques, consultez la section [Mesures collectées par l'agent CloudWatch](#) dans le guide de CloudWatch l'utilisateur Amazon.

Note

Les métriques de performance sont disponibles pour les versions 2.4.0 et ultérieures du pilote ENA (également pour la version 2.2.3). Le pilote ENA version 2.2.4 a été restauré en raison d'une dégradation potentielle des performances sur les instances EC2 de sixième génération. Nous vous recommandons de mettre à niveau vers la version actuelle du pilote afin de disposer des mises à niveau les plus récentes.

Voici quelques exemples d'utilisation des métriques de performance :

- Résoudre les problèmes de performance d'instance.
- Choisir la taille d'instance appropriée pour une charge de travail.
- Planifier de manière proactive des activités de mise à l'échelle.
- Définir des points de référence pour les applications afin de déterminer si elles optimisent les performances disponibles sur une instance.

Taux de rafraîchissement

Par défaut, le pilote actualise les métriques à l'aide d'un intervalle d'une seconde. Toutefois, l'application qui récupère les métriques peut utiliser un autre intervalle pour l'interrogation. Vous pouvez modifier l'intervalle d'actualisation dans le Gestionnaire de périphériques à l'aide des propriétés avancées du pilote.

Pour modifier l'intervalle d'actualisation des métriques du pilote Windows ENA, procédez comme suit :

1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.
2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.
6. Ouvrez l'onglet Avancé dans la fenêtre contextuelle.
7. Dans la liste Propriété, choisissez Intervalle d'actualisation des métriques pour modifier la valeur.
8. Une fois que vous avez terminé, choisissez OK.

réinitialisation du dispositif ENA

Le processus de réinitialisation démarre lorsque le pilote Windows ENA détecte une erreur sur une carte et marque la carte comme défectueuse. Le pilote ne peut pas se réinitialiser lui-même. C'est donc le système d'exploitation qui doit vérifier l'état de la carte et appeler la réinitialisation du pilote Windows ENA. Le processus de réinitialisation peut entraîner une perte de trafic pendant une brève période. Toutefois, les connexions TCP devraient pouvoir récupérer.

Le dispositif ENA peut également demander indirectement une procédure de réinitialisation du périphérique. Dans ce cas, il n'envoie pas de notification keep-alive. Par exemple, si le dispositif ENA atteint un état inconnu après le chargement d'une configuration irrécupérable, il peut arrêter d'envoyer des notifications keep-alive.

Causes courantes de réinitialisation du dispositif ENA

- Il manque des messages « keep-alive »

Le dispositif ENA publie des événements keep-alive selon une fréquence fixe (généralement une fois par seconde). Le pilote Windows ENA implémente un mécanisme de surveillance, qui recherche régulièrement la présence de ces messages keep-alive. S'il détecte un ou plusieurs nouveaux messages depuis la dernière vérification, il enregistre un résultat réussi. Sinon, le pilote conclut que le périphérique a subi une défaillance et lance une séquence de réinitialisation.

- Des paquets sont bloqués dans les files d'attente de transmission

Le dispositif ENA vérifie que les paquets circulent dans les files d'attente de transmission comme prévu. Le pilote Windows ENA détecte si les paquets sont bloqués et lance une séquence de réinitialisation le cas échéant.

- Délai d'attente des opérations de lecture pour les registres d'I/O mappées par la mémoire (MMIO)

Pour limiter les opérations de lecture des I/O mappées par la mémoire (MMIO), le pilote Windows ENA accède aux registres MMIO uniquement pendant les processus d'initialisation et de réinitialisation. Si le pilote détecte un délai d'attente, il effectue l'une des actions suivantes, en fonction du processus en cours d'exécution :

- Si un délai d'attente est détecté lors de l'initialisation, le flux échoue, ce qui fait que le pilote affiche un point d'exclamation jaune par le dispositif ENA dans le Gestionnaire de périphériques Windows.
- Si un délai d'attente est détecté lors de la réinitialisation, le flux échoue. Le système d'exploitation lance alors une suppression inattendue du dispositif ENA, puis le récupère en arrêtant et en démarrant le dispositif retiré. Pour plus d'informations sur la suppression inattendue d'une carte NIC, consultez [Gestion de la suppression inattendue d'une carte réseau](#) dans la documentation Microsoft Windows Hardware Developer.

Scénarios de résolution des problèmes

Les scénarios suivants peuvent vous aider à résoudre les problèmes potentiels liés au pilote Windows ENA. Nous vous recommandons de commencer la mise à niveau de votre pilote ENA si vous ne disposez pas de la dernière version. Pour trouver le pilote le plus récent pour la version de votre système d'exploitation Windows, consultez [pilote Windows ENA](#).

Version inattendue du pilote ENA installé

Description

Après avoir suivi les étapes d'installation d'une version spécifique du pilote ENA, le Gestionnaire de périphériques Windows indique que Windows a installé une version différente du pilote ENA.

Cause

Lorsque vous exécutez l'installation d'un package de pilotes, Windows classe tous les packages de pilotes valides pour le périphérique concerné dans le [magasin de pilotes](#) local avant qu'elle ne commence. Il sélectionne ensuite le package ayant la valeur de classement la plus faible comme étant le mieux adapté. Il peut être différent du package que vous aviez l'intention d'installer. Pour plus d'informations sur le processus de sélection du package de pilotes de périphériques, consultez [Comment Windows sélectionne un package de pilotes pour un périphérique](#) sur le site Web de documentation de Microsoft.

Solution

Pour vous assurer que Windows installe la version du package de pilotes que vous avez choisie, vous pouvez supprimer les packages de pilotes de rang inférieur du magasin de pilotes à l'aide de l'outil de ligne de commande [PnPUtil](#).

Pour mettre à jour le pilote ENA, procédez comme suit :

1. Connectez-vous à votre instance en tant qu'administrateur local.
2. Ouvrez la fenêtre Propriétés du Gestionnaire de périphériques, comme décrit dans la section [Vérifier l'état du dispositif ENA](#). L'onglet Général de la fenêtre Propriétés Amazon Elastic Network Adapter s'ouvre.
3. Ouvrez l'onglet Pilote.
4. Choisissez Mettre à jour le pilote. La boîte de dialogue Mettre à jour le logiciel du pilote – Amazon Elastic Network Adapter s'ouvre.

- a. Dans la section Comment voulez-vous rechercher le pilote ?, choisissez Rechercher un pilote sur mon ordinateur.
 - b. Sur la page Rechercher des pilotes sur votre ordinateur, choisissez Laissez-moi choisir dans une liste de pilotes de périphériques sur mon ordinateur, située sous la barre de recherche.
 - c. Sur la page Sélectionner le pilote de périphérique que vous voulez installer pour ce matériel, choisissez Je dispose d'un disque....
 - d. Dans la fenêtre Installer à partir du disque, choisissez Parcourir..., à côté de l'emplacement de fichier de la liste déroulante.
 - e. Naviguez jusqu'à l'emplacement où vous avez téléchargé le package du pilote ENA cible. Sélectionnez le fichier nommé `ena.inf` et choisissez Ouvrir.
 - f. Pour démarrer l'installation, cliquez sur OK, puis sur Suivant.
5. Si le programme d'installation ne redémarre pas automatiquement votre instance, exécutez l'`Restart-Computer PowerShell` applet de commande.

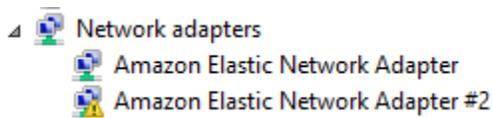
```
PS C:\> Restart-Computer
```

Avertissement de périphérique pour le pilote ENA

Description

L'icône du dispositif ENA dans la section Cartes réseau du Gestionnaire de périphériques affiche un panneau d'avertissement (triangle jaune avec un point d'exclamation à l'intérieur).

Voici un exemple de dispositif ENA avec l'icône d'avertissement dans le Gestionnaire de périphériques Windows :



Cause

Cet avertissement est généralement dû à des problèmes d'environnement, qui peuvent nécessiter plus de recherches et requièrent généralement un processus d'élimination pour déterminer la cause sous-jacente. Pour obtenir la liste complète des erreurs du périphérique, consultez [Gestionnaire de périphériques des messages d'erreur](#) dans la documentation Microsoft Windows Hardware Developer.

Solution

La solution à cet avertissement de périphérique dépend de la cause racine. Le processus d'élimination décrit ici comprend des étapes de base pour identifier et résoudre les problèmes les plus courants et pouvant être simples à résoudre. Une analyse supplémentaire des causes racines est nécessaire lorsque ces étapes ne résolvent pas le problème.

Suivez ces étapes pour essayer d'identifier et de résoudre les problèmes courants :

1. Arrêter et démarrer le périphérique

Ouvrez la fenêtre Propriétés du Gestionnaire de périphériques, comme décrit dans la section [Vérifier l'état du dispositif ENA](#). L'onglet Général de la fenêtre Propriétés de Amazon Elastic Network Adapter s'ouvre, et Statut de l'appareil affiche le code d'erreur et un court message.

- a. Ouvrez l'onglet Pilote.
- b. Choisissez Désactiver l'appareil, et répondez Oui au message d'avertissement qui s'affiche.
- c. Choisissez Activer l'appareil.

2. Arrêter et démarrer l'instance EC2

Si le dispositif affiche toujours l'icône d'avertissement dans le Gestionnaire de périphériques, arrêtez et démarrez l'instance EC2. Cette opération redémarre l'instance sur différents matériels dans la plupart des cas.

3. Examiner les problèmes possibles avec les ressources de l'instance

Si vous avez arrêté et démarré votre instance EC2 et que le problème persiste, cela peut indiquer un problème avec les ressources sur votre instance, comme une mémoire insuffisante.

Délai de connexion avec réinitialisation du dispositif (codes d'erreur 5007, 5205)

Description

L'Observateur d'événements Windows affiche le délai d'expiration du dispositif et les événements de réinitialisation qui se produisent conjointement pour les dispositifs ENA. Les messages ressemblent aux exemples suivants :

- Event ID 5007: Amazon Elastic Network Adapter : Timed out during an operation.
- Event ID 5205: Amazon Elastic Network Adapter : Adapter reset has been started.

Les réinitialisations du dispositif entraînent une perturbation minimale du trafic. Même lorsqu'il y a plusieurs réinitialisations, il serait inhabituel qu'elles provoquent une perturbation grave du réseau.

Cause

Cette séquence d'événements indique que le pilote Windows ENA a lancé une réinitialisation pour un dispositif ENA qui ne répondait pas. Toutefois, le mécanisme utilisé par le pilote de périphérique pour détecter ce problème est soumis à des faux positifs résultant d'une pénurie liée au processeur 0.

Solution

Si cette combinaison d'erreurs se produit souvent, vérifiez les allocations de ressources pour voir où des ajustements peuvent être utiles.

1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.
2. Pour ouvrir le Moniteur de ressources Windows, saisissez `resmon` dans la fenêtre Exécuter.
3. Choisissez OK. La fenêtre Moniteur de ressources s'ouvre alors.
4. Ouvrez l'onglet Processeur. Les graphiques d'utilisation par processeur s'affichent sur le côté droit de la fenêtre Moniteur de ressources.
5. Vérifiez les niveaux d'utilisation du processeur 0 pour voir s'ils sont trop élevés.

Nous vous recommandons de configurer RSS pour exclure le processeur 0 du dispositif ENA sur des types d'instance plus grands (plus de 16 vCPU). Pour les types d'instances plus petits, la configuration de RSS peut améliorer l'expérience, mais en raison du nombre inférieur de cœurs disponibles, des tests sont nécessaires pour s'assurer que la contrainte des cœurs CPU n'a pas d'impact négatif sur les performances.

Utilisez la commande `Set-NetAdapterRss` pour configurer le RSS pour votre dispositif ENA, comme illustré dans l'exemple suivant.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

La migration vers une infrastructure d'instance de sixième génération a un impact sur les performances ou les attachements

Description

Si vous migrez vers une instance EC2 de sixième génération, vous risquez de rencontrer des performances réduites ou des échecs d'attachements ENA si vous n'avez pas mis à jour la version de votre pilote Windows ENA.

Cause

Les types d'instances EC2 de sixième génération nécessitent la version minimale suivante du pilote Windows ENA, en fonction du système d'exploitation (OS) de l'instance.

Version minimale

Version Windows Server	Version de pilote ENA
Windows Server 2008 R2	2.2.3 ou 2.4.0
Windows Server 2012 et versions ultérieures	2.2.3 et ultérieures
Station de travail Windows	2.2.3 et ultérieures

Solution

Avant de passer à une instance EC2 de sixième génération, assurez-vous que l'AMI à partir de laquelle vous lancez dispose de pilotes compatibles basés sur le système d'exploitation de l'instance, comme indiqué dans le tableau précédent. Pour plus d'informations, consultez [Que dois-je faire avant de migrer mon instance EC2 vers une instance de sixième génération pour m'assurer de bénéficier de performances réseau optimales ?](#) dans le Centre de connaissances AWS re:Post .

Performances sous-optimales de l'interface réseau Elastic

Description

L'interface ENA ne fonctionne pas comme prévu.

Cause

L'analyse des causes racines des problèmes de performance est un processus d'élimination. Trop de variables sont impliquées pour nommer une cause commune.

Solution

La première étape de votre analyse des causes racines consiste à examiner les informations de diagnostic de l'instance qui ne fonctionne pas comme prévu afin de déterminer si des erreurs peuvent être à l'origine du problème. Pour plus d'informations, consultez la section [Collecter des informations de diagnostic sur l'instance](#).

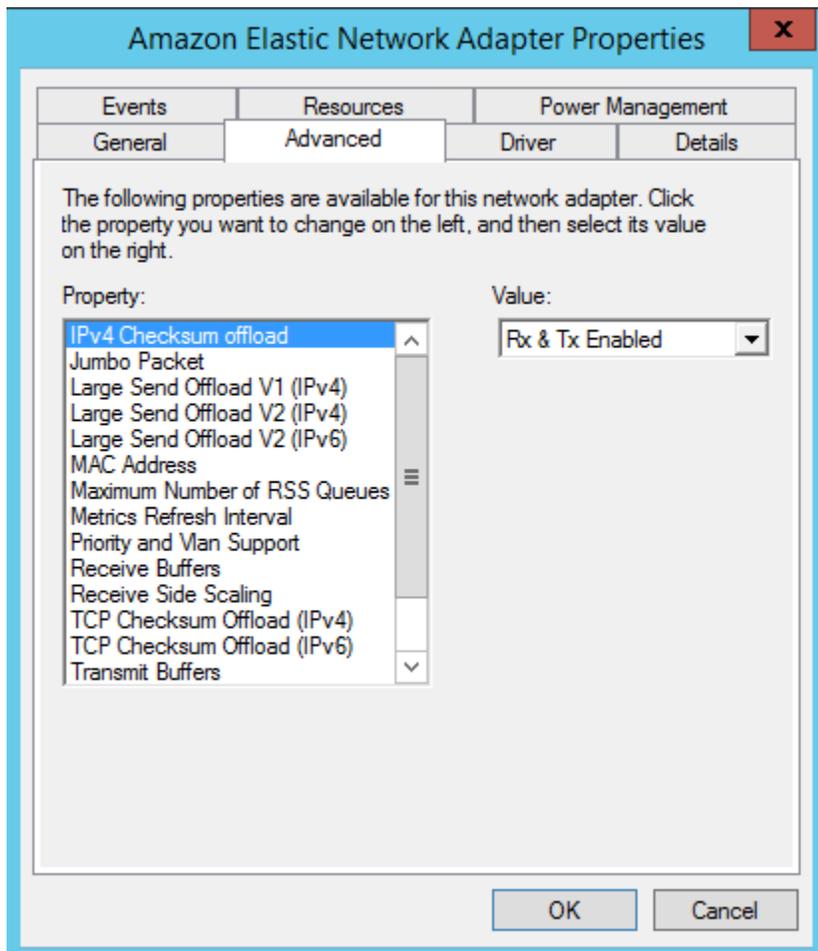
Il se peut que vous ayez besoin de modifier la configuration par défaut du système d'exploitation pour obtenir des performances réseau optimales sur les instances dont la mise en réseau est améliorée. Certaines optimisations, telles que l'activation du déchargement des totaux de contrôle et l'activation de RSS, sont configurées par défaut sur les AMI Windows officielles. Pour obtenir d'autres optimisations que vous pouvez appliquer au dispositif ENA, consultez les réglages de performance figurant dans [Réglages des performances du dispositif ENA](#).

Nous vous recommandons de procéder avec prudence et de limiter les modifications des propriétés de l'appareil à celles répertoriées dans cette section ou aux modifications spécifiques recommandées par l'équipe d' AWS assistance.

Pour modifier les propriétés du dispositif ENA, procédez comme suit :

1. Ouvrez Exécuter à l'aide de l'une des méthodes décrites dans la section précédente.
2. Pour ouvrir le Gestionnaire de périphériques Windows, saisissez `devmgmt.msc` la fenêtre Exécuter.
3. Choisissez OK. La fenêtre du Gestionnaire de périphériques s'ouvre.
4. Sélectionnez la flèche qui apparaît à gauche de Cartes réseau pour développer la liste.
5. Choisissez le nom ou ouvrez le menu contextuel pour Amazon Elastic Network Adapter, puis choisissez Propriétés. Cela ouvre la boîte de dialogue Propriétés d'Amazon Elastic Network Adapter.
6. Pour effectuer vos modifications, ouvrez l'onglet Avancé.
7. Lorsque vous avez terminé, sélectionnez OK pour enregistrer les modifications.

Voici un exemple de propriété du dispositif ENA dans le Gestionnaire de périphériques Windows :



Réglages des performances du dispositif ENA

Le tableau suivant inclut des propriétés pouvant être réglées pour améliorer les performances de l'interface ENA.

Entrée

Propriété	Description	Valeur par défaut	Ajustement
Tampons de réception	Contrôle le nombre d'entrées dans les files d'attente de réception du logiciel.	1 024	Peut être augmenté jusqu'à 8 192 au maximum.
Partage du trafic entrant (RSS)	Permet une distribution efficace du	Activées	Vous pouvez répartir la charge sur

Propriété	Description	Valeur par défaut	Ajustement
	traitement des réceptions réseau sur plusieurs processeurs dans des systèmes multiprocesseurs.		plusieurs processeurs. Pour en savoir plus, veuillez consulter la section Optimisation des performances réseau sur les instances Windows .

Propriété	Description	Valeur par défaut	Ajustement
Nombre maximal de files d'attente RSS	Définit le nombre maximum de files d'attente RSS autorisées lorsque RSS est activé.	32	<p>Le nombre de files d'attente RSS est déterminé lors de l'initialisation du pilote et inclut les limitations suivantes (entre autres) :</p> <ul style="list-style-type: none">• Limite de file d'attente RSS définie par cette propriété• Limites d'instance (nombre de vCPU)• <p>Limites de génération matérielle (jusqu'à 8 files d'attente RSS dans ENAv1 et jusqu'à 32 files d'attente RSS dans ENAv2)</p> <p>Vous pouvez définir une valeur entre 1 et 32, en fonction des limites de génération de votre instance et de votre matériel. Pour en savoir plus, veuillez consulter</p>

Propriété	Description	Valeur par défaut	Ajustement
			la section Optimisation des performances réseau sur les instances Windows .
Paquet jumbo	Permet l'utilisation de trames ethernet jumbo (plus de 1 500 octets de charge utile).	Désactivé (cela limite la charge utile à 1 500 octets)	La valeur peut être configurée sur 9015, ce qui se traduit par 9 001 octets de charge utile. Il s'agit de la charge utile maximale pour les trames ethernet jumbo. veuillez consulter Considérations relatives à l'utilisation de trames ethernet jumbo .

Considérations relatives à l'utilisation de trames ethernet jumbo

Les trames jumbo permettent d'utiliser plus de 1 500 octets de données en augmentant la charge utile par paquet, et donc en augmentant le pourcentage de paquet qui ne constitue pas des frais supplémentaires. Moins de paquets sont nécessaires pour envoyer le même volume de données utilisables. Toutefois, le trafic est limité à une MTU maximale de 1 500 dans les cas suivants :

- Trafic en dehors d'une AWS région donnée pour EC2 Classic.
- Trafic à l'extérieur d'un VPC unique.
- Trafic sur une connexion d'appairage de VPC entre régions.
- Trafic sur des connexions VPN.
- Trafic sur une passerelle Internet.

Note

Les paquets de plus de 1 500 octets sont fragmentés. Si vous avez l'indicateur `Don't Fragment` défini dans l'en-tête IP, ces paquets sont supprimés.

Les trames jumbo doivent être utilisées avec prudence pour le trafic Internet ou pour tout trafic quittant un VPC. Les paquets sont fragmentés par des systèmes intermédiaires, ce qui ralentit le trafic. Pour utiliser des trames jumbo à l'intérieur d'un VPC sans affecter le trafic sortant du VPC, essayez l'une des options suivantes :

- Configurez la taille MTU par acheminement.
- Utilisez plusieurs interfaces réseau avec différentes tailles MTU et différents acheminements.

Cas d'utilisation recommandés pour les trames jumbo

Les trames jumbo peuvent être utiles pour le trafic à l'intérieur et entre les VPC. Nous vous recommandons d'utiliser des trames jumbo pour les cas d'utilisation suivants :

- Pour les instances situées dans un même groupe de placement du cluster, les trames jumbo permettent d'atteindre le débit réseau maximum possible. Pour plus d'informations, consultez [Groupes de placement](#).
- Vous pouvez utiliser des trames jumbo pour le trafic entre vos VPC et vos réseaux sur site via AWS Direct Connect. Pour plus d'informations sur l'utilisation AWS Direct Connect et la vérification de la fonctionnalité des trames jumbo, voir [Définir le MTU réseau pour les interfaces virtuelles privées ou les interfaces virtuelles de transit dans le guide](#) de l'AWS Direct Connect utilisateur.
- Pour plus d'informations sur les tailles MTU prises en charge pour les passerelles de transit, consultez [Quotas pour vos passerelles de transit](#) dans Amazon VPC Transit Gateways.

Amélioration de la latence réseau pour les instances Amazon EC2 basées sur Linux

La latence réseau est le temps nécessaire à un paquet de données pour voyager de sa source à sa destination. Les applications qui envoient des données via le réseau ont besoin de réponses rapides pour offrir une expérience utilisateur positive. Une latence réseau élevée peut entraîner divers problèmes, tels que les suivants :

- Temps de chargement lents des pages Web
- Retard des flux vidéo
- Difficulté d'accès aux ressources en ligne

Cette section décrit les mesures que vous pouvez prendre pour améliorer la latence réseau sur les instances Amazon EC2 qui s'exécutent sous Linux. Afin d'obtenir une latence optimale, procédez comme suit pour configurer les paramètres de votre instance, de votre noyau et de votre pilote ENA. Pour obtenir des conseils de configuration supplémentaires, consultez le [guide des meilleures pratiques et d'optimisation des performances du pilote Linux ENA](#) sur GitHub.

Note

Les étapes et les paramètres peuvent varier légèrement en fonction de votre matériel réseau spécifique, de l'AMI à partir de laquelle vous avez lancé votre instance et du cas d'utilisation de votre application. Avant d'apporter des modifications, testez et surveillez minutieusement les performances de votre réseau pour vous assurer d'obtenir les résultats souhaités.

Réduction des sauts réseau

Chaque saut effectué par un paquet de données lorsqu'il passe d'un routeur à l'autre augmente la latence du réseau. En général, le trafic doit effectuer plusieurs sauts pour atteindre votre destination. Les deux méthodes permettant de réduire les sauts réseau de vos instances Amazon EC2 sont les suivantes :

- Groupe de placement du cluster : lorsque vous spécifiez un [groupe de placement du cluster](#), Amazon EC2 lance des instances qui sont à proximité les unes des autres, physiquement dans la même zone de disponibilité (AZ) avec une compression plus serrée. La proximité physique des instances du groupe leur permet de profiter d'une connectivité à haut débit, ce qui se traduit par une faible latence et un débit de flux unique élevé.
- Hôte dédié : un [hôte dédié](#) est un serveur physique qui vous est dédié. Avec un hôte dédié, vous pouvez lancer vos instances pour qu'elles s'exécutent sur le même serveur physique. La communication entre les instances qui s'exécutent sur le même hôte dédié peut se faire sans sauts réseau supplémentaires.

Configuration du noyau Linux

La configuration du noyau Linux peut augmenter ou diminuer la latence du réseau. Pour atteindre vos objectifs d'optimisation de la latence, il est important d'affiner la configuration du noyau Linux en fonction des exigences spécifiques de votre charge de travail.

Il existe de nombreuses options de configuration du noyau Linux qui peuvent contribuer à réduire la latence du réseau. Les options les plus efficaces sont les suivantes.

- Activer le mode d'interrogation occupé : le mode d'interrogation occupé réduit la latence sur le chemin de réception du réseau. Lorsque vous activez le mode d'interrogation occupé, le code de la couche de socket peut interroger directement la file d'attente de réception d'un périphérique réseau. L'inconvénient de l'interrogation intensive est l'utilisation accrue du CPU de l'hôte en raison de l'interrogation en boucle serrée des nouvelles données. Il existe deux paramètres globaux qui contrôlent le nombre de microsecondes d'attente des paquets pour toutes les interfaces.

busy_read

Un délai d'interrogation intensive de faible latence pour les lectures de sockets. Cela contrôle le nombre de microsecondes à attendre pour que la couche de socket lise les paquets dans la file d'attente du périphérique. Pour activer la fonction globalement avec la commande `sysctl`, l'organisation Linux Kernel recommande une valeur de 50 microsecondes. Pour plus d'informations, consultez [busy_read](#) dans le guide de l'utilisateur et de l'administrateur du noyau Linux.

```
$ C:\> sudo sysctl -w net.core.busy_read=50
```

busy_poll

Un délai d'interrogation intensive de faible latence pour poll et select. Cela contrôle le nombre de microsecondes à attendre pour que les événements se produisent. La valeur recommandée se situe entre 50 et 100 microsecondes, en fonction du nombre de sockets que vous interrogez. Plus vous ajoutez de sockets, plus la valeur doit être élevée.

```
$ C:\> sudo sysctl -w net.core.busy_poll=50
```

- Configurer les états d'alimentation « C-states » du processeur : les états « C-states » contrôlent les niveaux de veille dans lesquels un cœur peut entrer lorsqu'il est inutilisé. Il se peut que vous

voulez contrôler les états « C-state » pour ajuster la latence de votre système par rapport aux performances. Dans les états C profonds, le CPU est essentiellement « en veille » et ne peut pas répondre aux demandes jusqu'à ce qu'il se réveille et repasse à l'état actif. La mise en veille de cœurs prend du temps. Même si un cœur en veille donne plus de marge pour qu'un autre cœur fonctionne à une fréquence plus élevée, ce cœur en veille prend du temps pour se remettre en route et fonctionner.

Par exemple, si un cœur qui est assigné à la gestion des interruptions de paquets est en veille, il se peut que la prise en charge de cette interruption soit retardée. Vous pouvez configurer le système de manière à ce qu'il n'utilise pas d'états C profonds. Cependant, si cette configuration réduit la latence de réaction du processeur, elle réduit également la marge de manœuvre dont disposent les autres cœurs pour Turbo Boost.

Pour réduire la latence de réaction du processeur, vous pouvez limiter les états C-states plus approfondis. Pour plus d'informations, consultez la section [Performances élevées et faible latence en limitant les états C plus profonds](#) dans le guide de l'utilisateur Amazon Linux 2.

Configuration du pilote ENA

Le pilote réseau ENA permet la communication entre une instance et un réseau. Le pilote traite les paquets réseau et les transmet à la pile réseau ou à la carte Nitro. Lorsqu'un paquet réseau arrive, la carte Nitro génère une interruption pour le CPU afin d'informer le logiciel d'un événement.

Interruption

Une interruption est un signal qu'un périphérique ou une application envoie au processeur. L'interruption indique au processeur qu'un événement s'est produit ou qu'une condition qui a été remplie nécessite une attention immédiate. Les interruptions peuvent gérer des tâches sensibles au temps, telles que la réception de données d'une interface réseau, la gestion d'événements matériels ou le traitement de demandes émanant d'autres périphériques.

Modération des interruptions

La modération des interruptions est une technique qui réduit le nombre d'interruptions générées par un périphérique en les regroupant ou en les retardant. L'objectif de la modération d'interruptions est d'améliorer les performances du système en réduisant la surcharge associée à la gestion d'un grand nombre d'interruptions. Un trop grand nombre d'interruptions augmente l'utilisation du CPU, ce qui a un impact négatif sur le débit, tandis qu'un nombre insuffisant d'interruptions augmente la latence.

Modération dynamique des interruptions

La modération dynamique des interruptions est une forme améliorée de modération des interruptions qui ajuste dynamiquement le taux d'interruption en fonction de la charge actuelle du système et des modèles de trafic. Elle vise à trouver un équilibre entre la réduction du nombre d'interruptions et le nombre de paquets par seconde, ou bande passante.

Note

La modération dynamique des interruptions est activée par défaut dans certaines AMI (mais peut être activée ou désactivée dans toutes les AMI).

Pour minimiser la latence réseau, il peut être nécessaire de désactiver la modération des interruptions. Toutefois, cela peut également augmenter la charge de traitement des interruptions. Il est important de trouver le juste équilibre entre la réduction de la latence et la réduction de la charge. Les commandes `ethtool` peuvent vous aider à configurer la modération des interruptions. Par défaut, `rx-usecs` a la valeur de 20, et `tx-usecs` a la valeur 64.

Pour obtenir la configuration actuelle de modification des interruptions, utilisez la commande suivante.

```
$ C:\> ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on TX: off
rx-usecs: 20
tx-usecs: 64
```

Pour désactiver la modification des interruptions et la modération dynamique des interruptions, utilisez la commande suivante.

```
$ C:\> sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Considérations relatives au système Nitro pour le réglage des performances

Le Système Nitro est un ensemble de composants matériels et logiciels élaborés par AWS qui garantissent des performances élevées, une haute disponibilité et un niveau de sécurité élevé. Le système Nitro fournit des fonctionnalités similaires au bare metal qui éliminent les frais de virtualisation et prennent en charge les charges de travail qui nécessitent un accès complet au matériel hôte. Pour des informations plus détaillées, consultez [AWS Nitro System](#).

Tous les types d'instances EC2 de génération actuelle exécutent le traitement des paquets réseau sur les cartes Nitro EC2. Cette rubrique traite de la gestion des paquets de haut niveau sur la carte Nitro, des aspects courants de l'architecture et de la configuration du réseau qui ont un impact sur les performances de traitement des paquets, et des mesures que vous pouvez prendre pour optimiser les performances de vos instances basées sur Nitro.

Les cartes Nitro gèrent toutes les interfaces d'entrée et de sortie (E/S), telles que celles nécessaires aux clouds privés virtuels (VPC). Pour tous les composants qui envoient ou reçoivent des informations sur le réseau, les cartes Nitro agissent comme un dispositif informatique autonome pour le trafic d'E/S, physiquement distinct de la carte mère du système sur laquelle s'exécutent les charges de travail des clients.

Flux de paquets réseau sur les cartes Nitro

Les instances EC2 basées sur le système Nitro disposent de capacités d'accélération matérielle qui permettent un traitement des paquets plus rapide, tel que mesuré par le débit de paquets par seconde (PPS). Lorsqu'une carte Nitro effectue l'évaluation initiale d'un nouveau flux, elle enregistre des informations identiques pour tous les paquets du flux, telles que les groupes de sécurité, les listes de contrôle d'accès et les entrées des tables de routage. Lorsqu'il traite des paquets supplémentaires pour le même flux, il peut utiliser les informations enregistrées pour réduire la surcharge associée à ces paquets.

Votre débit de connexion est mesuré par la métrique des connexions par seconde (CPS). Chaque nouvelle connexion nécessite une surcharge de traitement supplémentaire qui doit être prise en compte dans les estimations de capacité de charge de travail. Il est important de prendre en compte à la fois les métriques CPS et PPS lorsque vous concevez vos charges de travail.

Comment établir une connexion

Lorsqu'une connexion est établie entre une instance basée sur Nitro et un autre point de terminaison, la carte Nitro évalue le flux complet du premier paquet envoyé ou reçu entre les deux points de terminaison. Pour les paquets suivants du même flux, une réévaluation complète n'est généralement pas nécessaire. Il existe toutefois des exceptions. Pour plus d'informations sur les exceptions, consultez [Paquets qui n'utilisent pas l'accélération matérielle](#).

Les propriétés suivantes définissent les deux points de terminaison et le flux de paquets entre eux. Ensemble, ces cinq propriétés sont connues sous le nom de flux à 5 tuples.

- IP Source

- Port source
- IP de destination
- Port de destination
- Protocole de communication

La direction du flux de paquets est appelée entrée (entrée) et sortie (sortie). Les descriptions de haut niveau suivantes résument le flux de paquets réseau de bout en bout.

- **Entrée** : lorsqu'une carte Nitro gère un paquet réseau entrant, elle l'évalue par rapport aux règles de pare-feu dynamiques et aux listes de contrôle d'accès. Il suit la connexion, la mesure et effectue d'autres actions, le cas échéant. Il transmet ensuite le paquet à sa destination sur le processeur hôte.
- **Sortie** : lorsqu'une carte Nitro gère un paquet réseau sortant, elle recherche la destination de l'interface distante, évalue diverses fonctions VPC, applique des limites de débit et effectue les autres actions applicables. Il transmet ensuite le paquet à sa destination de saut suivant sur le réseau.

Conception pour des performances optimales

Pour tirer parti des capacités de performance de votre système Nitro, vous devez comprendre quels sont vos besoins en matière de traitement réseau et comment ces besoins affectent la charge de travail de vos ressources Nitro. Vous pouvez ensuite concevoir des performances optimales pour votre environnement réseau. Les paramètres de votre infrastructure ainsi que la conception et la configuration de la charge de travail des applications peuvent avoir un impact à la fois sur le traitement des paquets et sur les taux de connexion. Par exemple, si votre application présente un taux d'établissement de connexion élevé, tel qu'un service DNS, un pare-feu ou un routeur virtuel, elle aura moins de chances de tirer parti de l'accélération matérielle qui ne se produit qu'une fois la connexion établie.

Vous pouvez configurer les paramètres d'application et d'infrastructure pour rationaliser les charges de travail et améliorer les performances du réseau. Cependant, tous les paquets ne sont pas éligibles à l'accélération. Le système Nitro utilise l'intégralité du flux réseau pour les nouvelles connexions et pour les paquets qui ne sont pas éligibles à l'accélération.

Le reste de cette section se concentrera sur les considérations relatives à la conception des applications et de l'infrastructure afin de garantir que les paquets circulent autant que possible selon le chemin accéléré.

Considérations

Lorsque vous configurez le trafic réseau pour votre instance, de nombreux aspects doivent être pris en compte qui peuvent affecter les performances du PPS. Une fois qu'un flux est établi, la majorité des paquets qui entrent ou sortent régulièrement sont éligibles à l'accélération. Cependant, des exceptions existent pour garantir que les conceptions d'infrastructure et les flux de paquets continuent de répondre aux normes du protocole.

Pour tirer le meilleur parti de votre carte Nitro, vous devez examiner attentivement les avantages et les inconvénients des détails de configuration suivants pour votre infrastructure et vos applications.

Considérations relatives aux infrastructures

La configuration de votre infrastructure peut affecter le flux de paquets et l'efficacité du traitement. La liste suivante inclut certaines considérations importantes.

Configuration de l'interface réseau avec asymétrie

Les groupes de sécurité utilisent le suivi des connexions pour suivre les informations relatives au trafic entrant et sortant de l'instance. Le routage asymétrique, selon lequel le trafic entre dans une instance via une interface réseau et en sort par une interface réseau différente, peut réduire les performances maximales qu'une instance peut atteindre si les flux sont suivis. Pour plus d'informations sur le suivi des connexions des groupes de sécurité, les connexions non suivies et les connexions suivies automatiquement, consultez [Suivi de connexion de groupe de sécurité](#).

Pilotes réseau

Les pilotes réseau sont régulièrement mis à jour et publiés. Si vos pilotes ne sont pas à jour, cela peut nuire considérablement aux performances. Maintenez vos pilotes à jour pour vous assurer que vous disposez des derniers correctifs et que vous pouvez tirer parti des améliorations de performances, telles que la fonction de trajectoire accélérée qui n'est disponible que pour la dernière génération de pilotes. Les pilotes antérieurs ne prennent pas en charge la fonction de trajectoire accélérée.

Pour tirer parti de la fonctionnalité de chemin accéléré, nous vous recommandons d'installer le dernier pilote ENA sur vos instances.

Instances Linux : pilote ENA Linux 2.2.9 ou version ultérieure. Pour installer ou mettre à jour le pilote ENA Linux depuis le GitHub référentiel Amazon Drivers, consultez la section [Compilation du pilote](#) du fichier readme.

Instances Windows : pilote Windows ENA 2.0.0 ou version ultérieure. Pour installer ou mettre à jour le pilote ENA pour Windows, voir [Installation du pilote Elastic Network Adapter \(ENA\)](#).

Distance entre les points de terminaison

Une connexion entre deux instances de la même zone de disponibilité peut traiter plus de paquets par seconde qu'une connexion entre régions en raison du fenêtrage TCP au niveau de la couche application, qui détermine la quantité de données pouvant être en vol à un moment donné. Les longues distances entre les instances augmentent la latence et diminuent le nombre de paquets que les points de terminaison peuvent traiter.

Considérations relatives à la conception de

Certains aspects de la conception et de la configuration des applications peuvent affecter l'efficacité de votre traitement. La liste suivante inclut certaines considérations importantes.

Taille du paquet

Des paquets de plus grande taille peuvent augmenter le débit des données qu'une instance peut envoyer et recevoir sur le réseau. Des paquets de plus petite taille peuvent augmenter le taux de traitement des paquets, mais cela peut réduire la bande passante maximale atteinte lorsque le nombre de paquets dépasse les tolérances PPS.

Si la taille d'un paquet dépasse l'unité de transmission maximale (MTU) d'un saut réseau, un routeur situé le long du chemin peut le fragmenter. Les fragments de paquets qui en résultent sont considérés comme des exceptions et sont traités au rythme standard (non accéléré). Cela peut entraîner des variations dans vos performances. Amazon EC2 prend en charge les trames jumbo de 9001 octets, mais tous les services ne le prennent pas en charge. Nous vous recommandons d'évaluer votre topologie lorsque vous configurez le MTU.

Compromis liés au protocole

Les protocoles fiables tels que le TCP sont plus gourmands que les protocoles peu fiables tels que le protocole UDP. La réduction de la surcharge et la simplification du traitement réseau pour le protocole de transport UDP peuvent entraîner un taux de PPS plus élevé, mais au détriment de la fiabilité de la distribution des paquets. Si la fiabilité de la livraison des paquets n'est pas essentielle pour votre application, le protocole UDP peut être une bonne option.

Micro-éclatement

La micro-explosion se produit lorsque le trafic dépasse les limites pendant de brèves périodes au lieu d'être réparti uniformément. Cela se produit généralement à l'échelle de la microseconde.

Supposons, par exemple, que vous disposiez d'une instance capable d'envoyer jusqu'à 10 Gbit/s et que votre application envoie la totalité des 10 Go en une demi-seconde. Cette micro-rafale dépasse la limite autorisée pendant la première demi-seconde et ne laisse rien pour le reste de la seconde. Même si vous avez envoyé 10 Go au cours de la période d'une seconde, les allocations pendant la première demi-seconde peuvent entraîner la mise en file d'attente ou le rejet de paquets.

Vous pouvez utiliser un planificateur réseau tel que Linux Traffic Control pour accélérer votre débit et éviter de provoquer des mises en file d'attente ou des pertes de paquets à la suite de microrafales.

Nombre de flux

Un flux unique est limité à 5 Gbit/s, sauf s'il fait partie d'un groupe de placement de clusters prenant en charge jusqu'à 10 Gbit/s, ou s'il utilise ENA Express, qui prend en charge jusqu'à 25 Gbit/s.

De même, une carte Nitro peut traiter un plus grand nombre de paquets sur plusieurs flux au lieu d'utiliser un seul flux. Pour atteindre le taux de traitement de paquets maximal par instance, nous recommandons d'utiliser au moins 100 flux sur les instances dont la bande passante cumulée est supérieure ou égale à 100 Gbit/s. À mesure que les capacités de bande passante agrégée augmentent, le nombre de flux nécessaires pour atteindre des taux de traitement de pointe augmente également. L'analyse comparative vous aidera à déterminer la configuration dont vous avez besoin pour atteindre des débits de pointe sur votre réseau.

Nombre de files d'attente d'Elastic Network Adapter (ENA)

Par défaut, le nombre maximum de files d'attente ENA est alloué à une interface réseau en fonction de la taille et du type de votre instance. La réduction du nombre de files d'attente peut réduire le taux de PPS maximal réalisable. Nous vous recommandons d'utiliser l'allocation de file d'attente par défaut pour de meilleures performances.

Pour Linux, une interface réseau est configurée avec le maximum par défaut. Pour les applications basées sur le Data Plane Development Kit (DPDK), nous vous recommandons de configurer le nombre maximum de files d'attente disponibles.

Fonctionnalité : surcharge du processus

Des fonctionnalités telles que Traffic Mirroring et ENA Express peuvent augmenter la charge de traitement, ce qui peut réduire les performances absolues de traitement des paquets. Vous pouvez limiter l'utilisation des fonctionnalités ou les désactiver pour augmenter les taux de traitement des paquets.

Suivi des connexions pour maintenir l'état

Vos groupes de sécurité utilisent le suivi des connexions pour stocker des informations sur le trafic à destination et en provenance de l'instance. Le suivi des connexions applique des règles à chaque flux individuel de trafic réseau afin de déterminer si le trafic est autorisé ou refusé. La carte Nitro utilise le suivi du flux pour maintenir l'état du flux. À mesure que de nouvelles règles de groupe de sécurité sont appliquées, davantage de travail est nécessaire pour évaluer le flux.

Note

Les flux de trafic réseau ne sont pas tous suivis. Si une règle de groupe de sécurité est configurée avec [Connexions non suivies](#), aucune tâche supplémentaire n'est requise, à l'exception des connexions qui sont automatiquement suivies pour garantir un routage symétrique lorsqu'il existe plusieurs chemins de réponse valides.

Paquets qui n'utilisent pas l'accélération matérielle

Tous les paquets ne peuvent pas tirer parti de l'accélération matérielle. La gestion de ces exceptions implique une certaine surcharge de traitement, nécessaire pour garantir l'intégrité de vos flux réseau. Les flux réseau doivent respecter de manière fiable les normes de protocole, se conformer aux modifications apportées à la conception du VPC et acheminer les paquets uniquement vers les destinations autorisées. Cependant, les frais généraux réduisent vos performances.

Fragments de paquets

Comme indiqué dans la section [Considérations relatives aux applications](#), les fragments de paquets résultant de paquets dépassant la MTU du réseau sont traités comme des exceptions et ne peuvent pas tirer parti de l'accélération matérielle.

Connexions inactives

Lorsqu'une connexion n'est pas active pendant un certain temps, même si le délai d'expiration de la connexion n'est pas atteint, le système peut annuler sa priorité. Ensuite, si les données arrivent après que la connexion n'a plus été priorisée, le système doit les traiter comme une exception pour pouvoir se reconnecter.

Pour gérer vos connexions, vous pouvez utiliser les délais de suivi des connexions pour fermer les connexions inactives. Vous pouvez également utiliser TCP keepalives pour maintenir ouvertes

les connexions inactives. Pour plus d'informations, consultez [Délai de suivi d'inactivité de la connexion](#).

Mutation VPC

Les mises à jour des groupes de sécurité, des tables de routage et des listes de contrôle d'accès doivent toutes être réévaluées dans le processus de traitement afin de garantir que les entrées de routage et les règles des groupes de sécurité s'appliquent toujours comme prévu.

Flux ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole de couche réseau utilisé par les périphériques réseau pour diagnostiquer les problèmes de communication réseau. Ces paquets utilisent toujours le flux complet.

Optimisez les performances du réseau sur votre système Nitro

Avant de prendre des décisions de conception ou d'ajuster les paramètres réseau de votre instance, nous vous recommandons de suivre les étapes suivantes pour obtenir les meilleurs résultats :

1. Comprenez les avantages et les inconvénients des mesures que vous pouvez prendre pour améliorer les performances en les évaluant [Considérations](#).

Pour en savoir plus et connaître les meilleures pratiques relatives à la configuration de votre instance, consultez :

Instances Linux — [Guide des meilleures pratiques et d'optimisation des performances du pilote Linux ENA](#) sur le GitHub site Web.

Instances Windows — [Meilleures pratiques pour la configuration des interfaces réseau](#).

2. Comparez vos charges de travail avec le nombre de flux actifs de pointe afin de déterminer une base de référence pour les performances de votre application. Avec une référence de performance, vous pouvez tester les variations de vos paramètres ou de la conception de votre application afin de déterminer quelles considérations auront le plus d'impact, en particulier si vous prévoyez de procéder à une mise à l'échelle ou à une extension externe.

La liste suivante contient les actions que vous pouvez effectuer pour optimiser les performances de votre PPS, en fonction des besoins de votre système.

- Réduisez la distance physique entre deux instances. Lorsque les instances d'envoi et de réception sont situées dans la même zone de disponibilité ou utilisent des groupes de placement de clusters, vous pouvez réduire le nombre de sauts qu'un paquet doit effectuer pour se déplacer d'un point de terminaison à un autre.
- Utilisez [Connexions non suivies](#).
- Utilisez le protocole UDP pour le trafic réseau.
- Pour les instances EC2 dont la bande passante cumulée est supérieure ou égale à 100 Gbit/s, répartissez la charge de travail sur au moins 100 flux individuels afin de répartir le travail de manière uniforme sur la carte Nitro.

Surveiller les performances sur les instances Linux

Vous pouvez utiliser les métriques Ethtool sur les instances Linux pour surveiller les indicateurs de performance réseau des instances tels que la bande passante, le débit de paquets et le suivi des connexions. Pour plus d'informations, consultez [Contrôlez les performances réseau de votre instance EC2](#).

Optimisation des performances réseau sur les instances Windows

Pour optimiser les performances réseau de vos instances Windows grâce à une mise en réseau améliorée, vous devrez peut-être modifier la configuration par défaut du système d'exploitation. Nous recommandons les modifications de configuration suivantes pour les applications nécessitant des performances réseau élevées. D'autres optimisations (telles que l'activation du déchargement par checksum et l'activation du flux RSS, par exemple) sont déjà configurées sur les AMI Windows officielles.

Note

Le transfert de la charge TCP Chimney doit être désactivé dans la plupart des cas d'utilisation ; il est obsolète depuis Windows Server 2016.

Outre ces optimisations de système d'exploitation, vous devez également tenir compte de l'unité de transmission maximale (MTU) de votre trafic réseau et l'ajuster en fonction de votre charge de travail et de l'architecture réseau. Pour plus d'informations, consultez [Unité de transmission maximale \(MTU\) du réseau pour votre instance EC2](#).

AWS mesure régulièrement les latences aller-retour moyennes entre les instances lancées dans un groupe de placement en cluster de 50 µs et les latences finales de 200 µs au 99,9 centile. Si vos applications nécessitent des temps de latence constamment faibles, nous vous recommandons d'utiliser la dernière version des pilotes ENA sur des instances à performances fixes et conçues sur le système Nitro.

Configuration de l'affinité d'UC RSS

La distribution de la charge de l'UC du trafic réseau sur plusieurs processeurs est exécutée à l'aide de la technologie RSS (Receive side scaling) Par défaut, les AMI officielles d'Amazon Windows sont configurées avec les RSS activés. Les ENI ENA fournissent jusqu'à huit files d'attente RSS. En paramétrant l'affinité de l'UC pour les files d'attente RSS, ainsi que d'autres processus, il est possible de répartir la charge de l'UC sur des systèmes multicœurs, permettant ainsi le traitement d'un trafic réseau plus important. Sur les types d'instance comportant plus de 16 vCPU, nous vous recommandons d'utiliser l'`Set-NetAdapterRSS` PowerShell applet de commande, qui exclut manuellement le processeur de démarrage (processeurs logiques 0 et 1 lorsque l'hyperthreading est activé) de la configuration RSS pour tous les ENI, afin d'éviter tout conflit avec les différents composants du système.

Windows prend en compte les hyper-threads et s'assure que les files d'attente RSS d'un même NIC sont toujours placées sur des cœurs physiques différents. Par conséquent, à moins que l'hyper-threading ne soit désactivé, afin d'éviter tout conflit avec d'autres cartes NIC, répartissez la configuration RSS de chaque carte NIC sur une plage de 16 processeurs logiques. L'`Set-NetAdapterRss` applet de commande vous permet de définir la plage par carte réseau des processeurs logiques valides en définissant les valeurs de `BaseProcessorGroup`, `BaseProcessorNumber` `MaxProcessingGroup` `MaxProcessorNumber`, et `NumaNode` (facultatif). S'il n'y a pas suffisamment de cœurs physiques pour éliminer complètement le conflit inter-NIC, minimiser le chevauchement des plages ou réduire le nombre de processeurs logiques dans les plages ENI en fonction de la charge de travail prévue de l'ENI (en d'autres termes, un réseau administratif à faible volume ENI peut ne pas avoir besoin d'autant de files RSS affectées). De plus, comme nous l'avons mentionné précédemment, divers composants doivent fonctionner sur le processeur 0, et nous recommandons donc de l'exclure de toutes les configurations RSS lorsque suffisamment de vCPU sont disponibles.

Par exemple, lorsqu'il y a trois ENI sur une instance de 72 vCPU avec 2 nœuds NUMA avec hyper-threading activé, les commandes suivantes répartissent la charge réseau entre les deux processeurs sans chevauchement et empêchent complètement l'utilisation du cœur 0.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -  
MaxProcessorNumber 16  
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -  
MaxProcessorNumber 14  
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -  
MaxProcessorNumber 30
```

Notez que ces paramètres sont persistants pour chaque adaptateur réseau. Si une instance est redimensionnée avec un nombre différent de vCPU, vous devez réévaluer la configuration RSS pour chaque ENI activé. La documentation complète de Microsoft pour l'applet de commande Set-NetAdapterRss est disponible ici : <https://docs.microsoft.com/en-us/powershell/module/netadapter/set-netadaptersrss>.

Remarque spécifique aux charges de travail SQL : nous vous recommandons également de revoir les paramètres d'affinité de vos threads d'I/O ainsi que votre configuration ENI RSS pour minimiser les conflits d'I/O et de réseau pour les mêmes processeurs. Consultez [Option de configuration de serveur de masque d'affinité](#).

Elastic Fabric Adapter

Elastic Fabric Adapter (EFA) est un périphérique réseau que vous pouvez attacher vos instances Amazon EC2 pour accélérer les applications de calcul haute performance (HPC) et machine learning. EFA vous permet d'atteindre les performances applicatives d'un cluster HPC sur site, grâce à l'évolutivité, à la flexibilité et à l'élasticité offertes par le cloud. AWS

Les EFA offrent une latence plus faible et plus cohérente avec un débit plus élevé que le transport TCP utilisé traditionnellement dans les systèmes HPC basés sur le cloud. Il améliore les performances des communications entre instances, ce qui est essentiel pour la mise à l'échelle des applications HPC et de Machine Learning. Il est optimisé pour fonctionner sur l'infrastructure AWS réseau existante et peut évoluer en fonction des exigences de l'application.

Les EFA s'intègrent à Libfabric 1.7.0 et aux versions ultérieures et prennent en charge Open MPI 5 et les versions ultérieures, ainsi que Intel MPI 2019 Update 5 et les versions ultérieures pour les applications HPC, et Nvidia Collective Communications Library (NCCL) pour les applications de machine learning.

Note

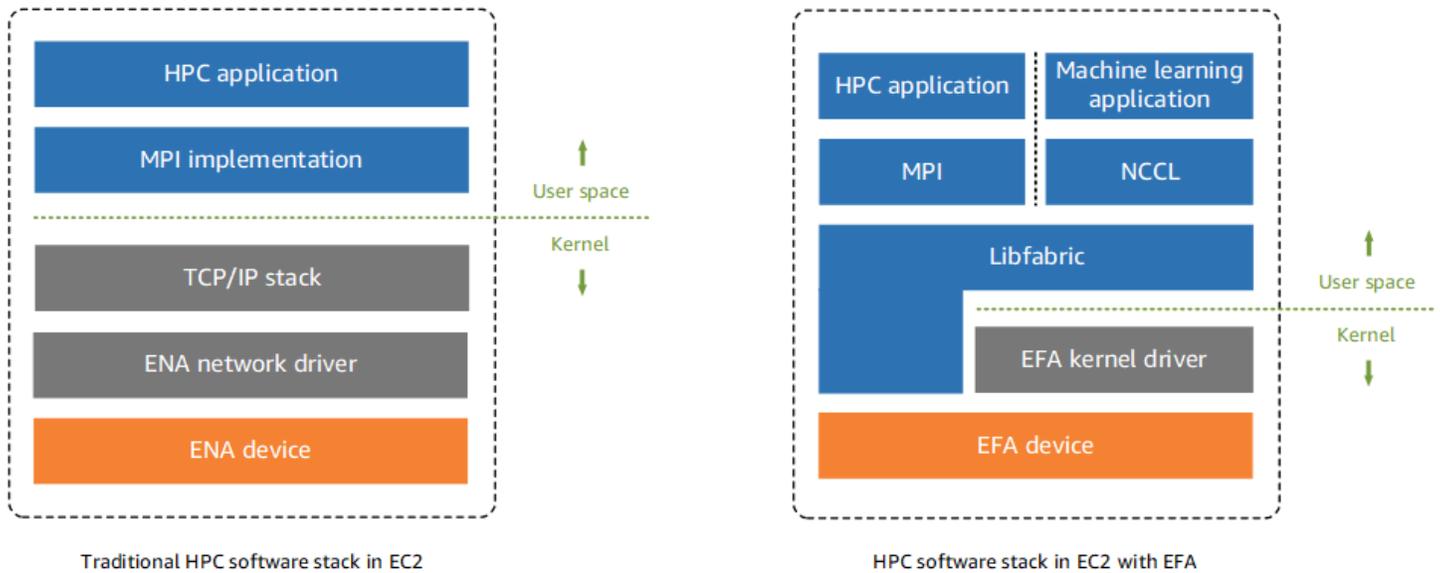
Les capacités de contournement du système d'exploitation d'EFA ne sont pas prises en charge sur des instances Windows. Si vous attachez un EFA à une instance Windows, l'instance fonctionne en tant qu'adaptateur Elastic Network Adapter sans les capacités EFA ajoutées.

Sommaire

- [Principes de base EFA](#)
- [Interfaces et bibliothèques prises en charge](#)
- [Types d'instance pris en charge](#)
- [Systèmes d'exploitation pris en charge](#)
- [Restrictions liées à EFA](#)
- [Tarification EFA](#)
- [Commencer à utiliser les instances P5 et EFA](#)
- [Commencer avec EFA et MPI](#)
- [Commencer avec EFA et NCCL](#)
- [Travailler avec EFA](#)
- [Surveillez un EFA](#)
- [Vérification du programme d'installation EFA à l'aide d'un total de contrôle](#)

Principes de base EFA

Un EFA est un adaptateur Elastic Network Adapter (ENA) avec des capacités ajoutées. Il offre toutes les fonctionnalités d'un ENA, avec des capacités de contournement du système d'exploitation supplémentaires. Le contournement du système d'exploitation est un modèle d'accès qui permet aux applications HPC et de Machine Learning de communiquer directement avec le matériel de l'interface réseau pour offrir des fonctionnalités de transport fiable à faible latence.



Traditionnellement, les applications HPC utilisent Message Passing Interface (MPI) pour servir d'interface avec le transport réseau du système. Dans le AWS cloud, cela signifie que les applications interagissent avec MPI, qui utilise ensuite la pile TCP/IP du système d'exploitation et le pilote de périphérique ENA pour permettre la communication réseau entre les instances.

Avec EFA, les applications HPC ou NCCL utilisent MPI pour servir d'interface avec l'API Libfabric. L'API Libfabric contourne le noyau du système d'exploitation et communique directement avec l'appareil EFA pour placer les paquets sur le réseau. Cela réduit la surcharge et permet à l'application HPC de s'exécuter plus efficacement.

Note

Libfabric est un composant essentiel du framework OpenFabrics Interfaces (OFI), qui définit et exporte l'API de l'espace utilisateur d'OFI. Pour plus d'informations, consultez le OpenFabrics site Web de [Libfabric](#).

Différences entre les EFAs et les adaptateurs ENA

Les adaptateurs Elastic Network Adapter (ENAs) fournissent les fonctions de réseaux IP classiques qui sont requises pour prendre en charge les réseaux VPC. Les EFA fournissent les mêmes fonctions de réseaux IP classiques que les ENA, mais ils prennent également en charge les capacités de contournement du système d'exploitation. Le contournement du système d'exploitation permet aux applications HPC et de Machine Learning de contourner le noyau du système d'exploitation et de communiquer directement avec l'appareil EFA.

Interfaces et bibliothèques prises en charge

Les EFA prennent en charge les interfaces et bibliothèques suivantes :

- Open MPI 5 et versions ultérieures
- Une version Open MPI 4.0 ou plus récente est privilégiée pour Graviton
- Intel MPI 2019 Update 5 et ultérieure
- NVIDIA Collective Communications Library (NCCL) 2.4.2 et versions ultérieures

Types d'instance pris en charge

Les types d'instance suivants prennent en charge EFAs :

- Usage général : m5dn.24xlarge m5dn.metal m5n.24xlarge | m5n.metal | m5zn.12xlarge | m5zn.metal m6a.48xlarge | m6a.metal | m6i.32xlarge | m6i.metal | m6id.32xlarge | m6id.metal | m6idn.32xlarge m6idn.metal | m6in.32xlarge | m6in.metal | m7a.48xlarge | m7a.metal-48xl | m7g.16xlarge m7g.metal | m7gd.16xlarge | m7gd.metal | m7i.48xlarge | m7i.metal-48xl
- Optimisé pour le calcul : c5n.9xlarge c5n.18xlarge c5n.metal c6a.48xlarge | c6a.metal | c6gn.16xlarge | c6i.32xlarge | c6i.metal c6id.32xlarge | c6id.metal | c6in.32xlarge | c6in.metal | c7a.48xlarge | c7a.metal-48xl | c7g.16xlarge | c7g.metal | c7gd.16xlarge | c7gd.metal | c7gn.16xlarge | c7gn.metal | c7i.48xlarge | c7i.metal-48xl
- Mémoire optimisée : r5dn.24xlarge | r5dn.metal | r5n.24xlarge | r5n.metal | r6a.48xlarge | r6a.metal | r6i.32xlarge | r6i.metal | r6idn.32xlarge | r6idn.metal | r6in.32xlarge | r6in.metal | r6id.32xlarge | r6id.metal | r7a.48xlarge | r7a.metal-48xl | r7g.16xlarge | r7g.metal | r7gd.16xlarge | r7gd.metal | r7i.48xlarge | r7i.metal-48xl | r7iz.32xlarge | r7iz.metal-32xl | u7i-12tb.224xlarge | u7in-16tb.224xlarge | u7in-24tb.224xlarge | u7in-32tb.224xlarge | x2idn.32xlarge | x2idn.metal | x2iedn.32xlarge | x2iedn.metal | x2iezn.12xlarge | x2iezn.metal
- Stockage optimisé : i3en.12xlarge | i3en.24xlarge | i3en.metal | i4g.16xlarge | i4i.32xlarge | i4i.metal | im4gn.16xlarge
- Calcul accéléré : dl1.24xlarge dl2q.24xlarge | g4dn.8xlarge | g4dn.12xlarge | g4dn.16xlarge | g4dn.metal | g5.8xlarge | g5.12xlarge | g5.16xlarge | g5.24xlarge

g5.48xlarge | g6.8xlarge | g6.12xlarge | g6.16xlarge | g6.24xlarge | g6.48xlarge
| gr6.8xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge |
p5.48xlarge | trn1.32xlarge | trn1n.32xlarge | vt1.24xlarge

- Informatique haute performance : hpc6a.48xlarge hpc6id.32xlarge | hpc7a.12xlarge
| | hpc7a.24xlarge | hpc7a.48xlarge | hpc7a.96xlarge | hpc7g.4xlarge |
hpc7g.8xlarge | hpc7g.16xlarge

Pour consulter les types d'instance disponibles qui prennent en charge les EFA dans une région spécifique

Les types d'instance disponibles varient selon la région. Pour consulter les types d'instance disponibles qui prennent en charge les EFA dans une région, utilisez la commande [describe-instance-types](#) avec le paramètre `--region`. Incluez le paramètre `--filters` pour étendre les résultats aux types d'instance qui prennent en charge EFA et le paramètre `--query` pour étendre la sortie à la valeur de `InstanceType`.

```
aws ec2 describe-instance-types --region us-east-1 --filters Name=network-info.efa-supported,Values=true --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Systèmes d'exploitation pris en charge

Les systèmes d'exploitation suivants prennent en charge les EFA avec les types d'instance Intel/AMD x86 :

- Amazon Linux 2023
- Amazon Linux 2
- CentOS 7
- RHEL 7, 8 et 9
- Debian 10 et 11
- Rocky Linux 8 et 9
- Ubuntu 20.04 et 22.04
- SUSE Linux Enterprise 15 SP2 ou version ultérieure
- OpenSUSE Leap 15.4 et versions ultérieures

Note

Ubuntu 20.04 prend en charge l'assistance directe entre pairs lorsqu'il est utilisé avec les instances d11.24xlarge.

Les systèmes d'exploitation suivants prennent en charge les EFA avec les types d'instance ARM (Graviton) :

- Amazon Linux 2023
- Amazon Linux 2
- RHEL 8/9 et Rocky Linux 8/9
- Debian 10 et 11
- Ubuntu 20.04 et 22.04
- SUSE Linux Enterprise 15 SP2 ou version ultérieure

Restrictions liées à EFA

Les EFA présentent les limitations suivantes :

- Tous les types d'instance P4 et P5 prennent en charge l'accès direct à la mémoire à distance (RDMA) NVIDIA GPUDirect.
- Le trafic EFA entre les instances P4d/P4de/DL1 et les autres types d'instances n'est actuellement pas pris en charge.
- [Les types d'instance qui prennent en charge plusieurs cartes réseau](#) peuvent être configurés avec un EFA par carte réseau. Tous les autres types d'instance pris en charge ne prennent en charge qu'un EFA par instance.
- Pour c7g.16xlarge, m7g.16xlarge et r7g.16xlarge les instances dédiées et les hôtes dédiés ne sont pas pris en charge lorsqu'un EFA est attaché.
- Le trafic de contournement du système d'exploitation EFA est limité à un seul sous-réseau. En d'autres termes, le trafic EFA ne peut pas être envoyé d'un sous-réseau à un autre. Le trafic IP normal de l'EFA peut être envoyé d'un sous-réseau à un autre.
- Le trafic de contournement du système d'exploitation EFA n'est pas routable. Le trafic IP normal de l'EFA reste routable.

- L'EFA doit appartenir à un groupe de sécurité qui autorise tout le trafic entrant et sortant vers et depuis le groupe de sécurité proprement dit.
- L'EFA n'est pas pris en charge sur les instances Windows.
- L'EFA n'est pas pris en charge sur AWS [Outposts](#).

Tarifification EFA

EFA est disponible en tant que fonctionnalité de mise en réseau Amazon EC2 optionnelle que vous pouvez activer sur n'importe quelle instance prise en charge sans frais supplémentaires.

Commencer à utiliser les instances P5 et EFA

Les instances P5 fournissent 3 200 Gbit/s de bande passante du réseau en utilisant plusieurs interfaces EFA. Les instances P5 prennent en charge 32 cartes réseau. Pour plus d'informations sur la mise en route avec des instances P5, veuillez consulter [Commencez avec les instances P5 pour Linux](#).

Nous vous recommandons de définir une seule interface réseau EFA par carte réseau. Pour configurer ces interfaces au lancement, nous vous recommandons d'utiliser les paramètres suivants :

- Pour l'interface réseau 0, spécifiez l'index d'appareils 0.
- Pour les interfaces réseaux 1 à 31, spécifiez l'index d'appareils 1.

Si vous utilisez la console Amazon EC2, dans l'assistant Lancement d'instance, choisissez Modifier dans la section Réglages réseau. Développez Configuration réseau avancée et choisissez Ajouter une interface réseau pour ajouter le nombre requis d'interfaces réseau. Pour chaque interface réseau, pour EFA, sélectionnez Activer. Pour toutes les interfaces réseau, à l'exception de l'interface réseau principale, pour Index d'appareils, spécifiez 1. Configurez les paramètres restants selon les besoins.

Si vous utilisez la commande [run-instances AWS CLI](#), pour `--network-interfaces`, spécifiez le nombre requis d'interfaces réseau. Pour chaque interface réseau, pour `InterfaceType`, spécifiez `e-fa`. Pour l'interface réseau principale, pour `NetworkCardIndex` et `DeviceIndex`, spécifiez 0. Pour les autres interfaces réseau, pour `NetworkCardIndex`, spécifiez une valeur unique comprise entre 1 et 31, et pour `DeviceIndex`, spécifiez 1.

L'exemple d'extrait de commande suivant montre une demande avec 32 interfaces réseau EFA.

```
$ aws --region $REGION ec2 run-instances \  
--instance-type p5.48xlarge \  
--count 1 \  
--key-name key_pair_name \  
--image-id ami_id \  
--network-interfaces  
"NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa-  
\  
"
```

```
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  
"NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\  

```

```

"NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
...

```

Si vous utilisez un modèle de lancement, spécifiez le nombre requis d'interfaces réseau dans le modèle de lancement. Pour chaque interface réseau, pour `InterfaceType`, spécifiez `efa`. Pour l'interface réseau principale, pour `NetworkCardIndex` et `DeviceIndex`, spécifiez `0`. Pour les autres interfaces réseau, pour `NetworkCardIndex`, spécifiez une valeur unique comprise entre 1 et 31, et pour `DeviceIndex`, spécifiez 1. L'extrait de code suivant montre un exemple avec 3 interfaces réseau sur 32 possibles.

```

"NetworkInterfaces":[
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 1,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,

```

```
"Groups": [
  "security_group_id"
],
"DeleteOnTermination": true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress": false,
  "Groups": [
    "security_group_id"
  ],
  "DeleteOnTermination": true
}
...
```

Lorsque vous lancez une instance P5 avec plusieurs interfaces réseau, vous ne pouvez pas attribuer automatiquement des adresses IP publiques. Toutefois, vous pouvez associer une adresse IP élastique à l'interface réseau principale (NetworkCardIndex=0, DeviceIndex =0) après le lancement pour la connectivité Internet. Ubuntu 20.04 et versions ultérieures et Amazon Linux 2 et versions ultérieures sont configurés pour utiliser l'interface réseau principale pour le trafic Internet lorsque l'instance est lancée, comme recommandé ci-dessus.

Commencer avec EFA et MPI

Ce didacticiel vous permet de lancer un cluster d'instances EFA et compatible MPI pour les charges de travail HPC. Dans ce didacticiel, vous exécuterez les étapes suivantes :

Sommaire

- [Étape 1 : Préparer un groupe de sécurité activé pour les EFA](#)
- [Étape 2 : Lancer une instance temporaire](#)
- [Étape 3 : Installer le logiciel EFA](#)
- [Étape 4 : \(Facultatif\) Activer Open MPI 5](#)
- [Étape 5 : \(Facultatif\) Installer Intel MPI](#)
- [Étape 6 : Désactiver la protection ptrace](#)
- [Étape 7. Confirmer l'installation](#)
- [Étape 8 : Installer votre application HPC](#)

- [Étape 9 : Créer une AMI activée pour EFA](#)
- [Étape 10 : Lancer des instances activées pour EFA dans un groupe de placement du cluster](#)
- [Étape 11 : Résilier l'instance temporaire](#)
- [Étape 12 : Activer SSH sans mot de passe](#)

Étape 1 : Préparer un groupe de sécurité activé pour les EFA

Un EFA a besoin d'un groupe de sécurité qui autorise tout le trafic entrant et sortant vers et depuis le groupe de sécurité proprement dit. La procédure suivante crée un groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance de lui-même, et qui autorise le trafic SSH entrant depuis n'importe quelle adresse IPv4 pour la connectivité SSH.

Important

Ce groupe de sécurité n'est destiné qu'à des fins de test. Pour vos environnements de production, nous vous recommandons de créer une règle SSH entrante qui autorise le trafic uniquement à partir de l'adresse IP à partir de laquelle vous vous connectez, telle que l'adresse IP de votre ordinateur ou une plage d'adresses IP de votre réseau local.

Pour d'autres scénarios, consultez [Règles de groupe de sécurité pour différents cas d'utilisation](#).

Pour créer un groupe de sécurité activé pour EFA

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité), puis Create security group (Créer un groupe de sécurité).
3. Dans la fenêtre Create security group (Créer un groupe de sécurité), procédez comme suit :
 - a. Pour Nom du groupe de sécurité, saisissez un nom descriptif pour le groupe de sécurité, tel que EFA-enabled security group.
 - b. (Facultatif) Pour Description, saisissez une brève description du groupe de sécurité.
 - c. Pour VPC, sélectionnez le VPC dans lequel vous prévoyez de lancer vos instances activées pour EFA.
 - d. Sélectionnez Create security group (Créer un groupe de sécurité).

4. Sélectionnez le groupe de sécurité que vous avez créé et dans l'onglet Details (Détails), copiez le Security group ID (ID du groupe de sécurité).
5. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit inbound rules (Modifier les règles entrantes), puis procédez comme suit :
 - a. Choisissez Ajouter une règle.
 - b. Pour Type, sélectionnez Tout le trafic.
 - c. Pour Source type (Type de source), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.
 - d. Choisissez Ajouter une règle.
 - e. Pour Type, choisissez SSH.
 - f. Pour Source type (Type de source), choisissez Anywhere-IPv4 (IPv4 n'importe où).
 - g. Sélectionnez Enregistrer les règles.
6. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit outbound rules (Modifier les règles sortantes), puis procédez comme suit :
 - a. Choisissez Ajouter une règle.
 - b. Pour Type, sélectionnez Tout le trafic.
 - c. Pour Destination type (Type de destination), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.
 - d. Sélectionnez Enregistrer les règles.

Étape 2 : Lancer une instance temporaire

Lancez une instance temporaire que vous pouvez utiliser pour installer et configurer les composants logiciels EFA. Vous utilisez cette instance pour créer une AMI activée pour EFA depuis laquelle vous pouvez lancer vos instances activées pour EFA.

Pour lancer une instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.

3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que `EFA-instance`. Le nom est attribué à l'instance en tant qu'identification de ressource (Name=`EFA-instance`).
4. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez une AMI pour l'un des [systèmes d'exploitation pris en charge](#).
5. Dans la section Instance type (Type d'instance), sélectionnez un [type d'instance pris en charge](#).
6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :
 - a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez pas de sous-réseau, vous ne pouvez pas activer l'instance pour EFA.
 - b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.
 - c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).
8. Dans la section Storage (Stockage), configurez les volumes selon vos besoins.
9. Dans le panneau Summary (Récapitulatif) à droite, choisissez Launch instance (Lancer l'instance).

Étape 3 : Installer le logiciel EFA

Installez le noyau activé pour EFA, les pilotes EFA, Libfabric et la pile Open MPI requis pour prendre en charge EFA sur votre instance temporaire.

Les étapes varient selon que vous avez l'intention d'utiliser EFA avec Open MPI ou avec Intel MPI, ou avec Open MPI et Intel MPI.

Pour installer le logiciel EFA

1. Connectez-vous à l'instance que vous avez lancée. Pour plus d'informations, consultez [Connectez-vous à votre instance Linux](#).
2. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance. Ce processus peut prendre quelques minutes.

- Amazon Linux 2023, Amazon Linux 2, RHEL 7/8/9, CentOS 7, Rocky Linux 8/9

```
$ sudo yum update -y
```

- Ubuntu 20.04/22.04 et Debian 10/11

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

- SUSE Linux Enterprise

```
$ sudo zypper update -y
```

3. Redémarrez l'instance et reconnectez-vous à celle-ci.
4. Téléchargez les fichiers d'installation du logiciel EFA. Les fichiers d'installation du logiciel sont packagés dans un fichier d'archive compressé (.tar.gz). Pour télécharger la version stable la plus récente, utilisez la commande suivante.

```
$ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz
```

Vous pouvez aussi obtenir la dernière version en remplaçant le numéro de version par `latest` dans la commande ci-dessus.

5. (Facultatif) Vérifiez l'authenticité et l'intégrité du fichier tarball EFA (.tar.gz).

Nous vous recommandons de le faire pour vérifier l'identité de l'éditeur du logiciel et pour vérifier que le fichier n'a pas été modifié ou endommagé depuis sa publication. Si vous ne souhaitez pas vérifier le fichier d'archive, ignorez cette étape.

Note

Sinon, si vous préférez vérifier le fichier d'archive à l'aide d'un total de contrôle MD5 ou SHA256 à la place, consultez [Vérification du programme d'installation EFA à l'aide d'un total de contrôle](#).

- a. Téléchargez la clé publique GPG et importez-la dans votre porte-clés.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --import aws-efa-installer.key
```

La commande doit renvoyer une valeur clé. Notez la valeur clé, car vous en aurez besoin lors de l'étape suivante.

- b. Vérifiez l'empreinte digitale de la clé GPG. Exécutez la commande suivante et spécifiez la valeur clé que vous avez obtenue à l'étape précédente.

```
$ gpg --fingerprint key_value
```

La commande doit renvoyer une empreinte digitale identique à 4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC. Si l'empreinte digitale ne correspond pas, n'exécutez pas le script d'installation EFA et contactez AWS Support.

- c. Téléchargez le fichier SIGNATURE et vérifiez la signature du fichier d'archive EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz.sig && gpg --verify ./aws-efa-installer-1.32.0.tar.gz.sig
```

Voici un exemple de sortie.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC
```

Si le résultat inclut `Good signature` et que l'empreinte digitale correspond à l'empreinte digitale renvoyée à l'étape précédente, passez à l'étape suivante. Si ce n'est pas le cas, n'exécutez pas le script d'installation EFA et contactez AWS Support.

6. Procédez à l'extraction des fichiers à partir du fichier compressé `.tar.gz` et accédez au répertoire extrait.

```
$ C:\> tar -xf aws-efa-installer-1.32.0.tar.gz && cd aws-efa-installer
```

7. Installez le logiciel EFA. Effectuez l'une des actions suivantes en fonction de votre cas d'utilisation.

Note

EFA ne prend pas en charge NVIDIA GPUDirect avec SUSE Linux. Si vous utilisez SUSE Linux, vous devez également spécifier l'option `--skip-kmod` pour empêcher l'installation de `kmod`. Par défaut, SUSE Linux n'autorise pas les modules out-of-tree du noyau.

Open MPI and Intel MPI

Si vous avez l'intention d'utiliser EFA avec Open MPI et Intel MPI, vous devez installer le logiciel EFA avec Libfabric et Open MPI, et vous devez réaliser l'Étape 5 : Installer Intel MPI.

Pour installer le logiciel EFA avec Libfabric et Open MPI, exécutez la commande suivante.

Note

Depuis EFA 1.30.0, Open MPI 4 et Open MPI 5 sont installés par défaut. Vous pouvez éventuellement spécifier la version d'Open MPI que vous souhaitez installer. Pour installer uniquement Open MPI 4, incluez `--mpi=openmpi4`. Pour installer uniquement Open MPI 5, incluez `--mpi=openmpi5`. Pour installer les deux, omettez l'option `--mpi`.

```
$ C:\> sudo ./efa_installer.sh -y
```

Libfabric est installé dans `/opt/amazon/efa`. Open MPI 4 est installé dans `/opt/amazon/openmpi`. Open MPI 5 est installé dans `/opt/amazon/openmpi5`.

Open MPI only

Si vous avez l'intention d'utiliser EFA avec Open MPI uniquement, vous devez installer le logiciel EFA avec Libfabric et Open MPI, et vous pouvez ignorer l'Étape 5 : Installer Intel MPI. Pour installer le logiciel EFA avec Libfabric et Open MPI, exécutez la commande suivante.

Note

Depuis EFA 1.30.0, Open MPI 4 et Open MPI 5 sont installés par défaut. Vous pouvez éventuellement spécifier la version d'Open MPI que vous souhaitez installer. Pour installer uniquement Open MPI 4, incluez `--mpi=openmpi4`. Pour installer uniquement Open MPI 5, incluez `--mpi=openmpi5`. Pour installer les deux, omettez l'option `--mpi`.

```
$ C:\> sudo ./efa_installer.sh -y
```

Libfabric est installé dans `/opt/amazon/efa`. Open MPI 4 est installé dans `/opt/amazon/openmpi`. Open MPI 5 est installé dans `/opt/amazon/openmpi5`.

Intel MPI only

Si vous avez l'intention d'utiliser EFA uniquement avec Intel MPI, vous pouvez installer le logiciel EFA sans Libfabric ni Open MPI. Dans ce cas, Intel MPI utilise son Libfabric intégré. Si vous optez pour cette solution, vous devez réaliser l'Étape 5 : Installer Intel MPI.

Pour installer le logiciel EFA sans Libfabric ni Open MPI, exécutez la commande suivante.

```
$ C:\> sudo ./efa_installer.sh -y --minimal
```

8. Si le programme d'installation d'EFA vous invite à redémarrer l'instance, faites-le et reconnectez-vous à l'instance. Sinon, déconnectez-vous de l'instance, puis reconnectez-vous pour terminer l'installation.

Étape 4 : (Facultatif) Activer Open MPI 5**Note**

Vous ne devez effectuer cette étape que si vous avez l'intention d'utiliser Intel MPI 5.

Depuis EFA 1.30.0, Open MPI 4 et Open MPI 5 sont installés par défaut. Vous pouvez également choisir d'installer uniquement Open MPI 4 ou Open MPI 5.

Si vous avez choisi d'installer Open MPI 5 à l'Étape 3 : Installer le logiciel EFA et que vous avez l'intention de l'utiliser, vous devez effectuer les étapes suivantes pour l'activer.

Activation d'Open MPI 5

1. Ajoutez Open MPI 5 à la variable d'environnement PATH.

```
$ module load openmpi5
```

2. Vérifiez qu'Open MPI 5 est activé pour être utilisé.

```
$ which mpicc
```

La commande doit renvoyer le répertoire d'installation Open MPI 5 : `/opt/amazon/openmpi5`.

3. (Facultatif) Pour vous assurer qu'Open MPI 5 est ajouté à la variable d'environnement PATH à chaque démarrage de l'instance, procédez comme suit :

bash shell

Ajoutez `module load openmpi5` à `/home/username/.bashrc` et `/home/username/.bash_profile`.

csh and tcsh shells

Ajoutez `module load openmpi5` à `/home/username/.cshrc`.

Si vous devez supprimer Open MPI 5 de la variable d'environnement PATH, exécutez la commande suivante et supprimez-la des scripts de démarrage du shell.

```
$ module unload openmpi5
```

Étape 5 : (Facultatif) Installer Intel MPI

Important

Vous ne devez effectuer cette étape que si vous avez l'intention d'utiliser Intel MPI. Si vous avez l'intention d'utiliser uniquement Open MPI, passez cette étape.

Intel MPI nécessite une installation et une configuration de variable d'environnement supplémentaires.

Prérequis

Vérifiez que l'utilisateur qui exécute les étapes suivantes dispose des autorisations sudo.

Pour installer Intel MPI

1. Pour télécharger le script d'installation d'Intel MPI, procédez comme suit :
 - a. Visitez le [site web d'Intel](#).
 - b. Dans la section Intel MPI Library (Bibliothèque MPI Intel) de la page web, choisissez le lien du programme d'installation Offline (Hors ligne) de Intel MPI Library for Linux.
2. Exécutez le script d'installation que vous avez téléchargé à l'étape précédente.

```
$ C:\> sudo bash installation_script_name.sh
```

3. Dans le programme d'installation, choisissez Accept & install (Accepter et installer).
4. Lisez le programme Intel Improvement Program, choisissez l'option appropriée, puis choisissez Begin Installation (Démarrer l'installation).
5. Une fois l'installation terminée, choisissez Fermer.
6. Par défaut, Intel MPI utilise sa bibliothèque embarquée (interne) Libfabric. Vous pouvez configurer Intel MPI pour qu'il utilise plutôt la bibliothèque Libfabric livrée avec le programme d'installation d'EFA. Généralement, le programme d'installation d'EFA est livré avec une version de Libfabric plus récente que celle d'Intel MPI. Dans certains cas, la bibliothèque Libfabric fournie avec le programme d'installation d'EFA est plus performante que celle d'Intel MPI. Pour configurer Intel MPI afin qu'il utilise la bibliothèque Libfabric fournie avec le programme d'installation d'EFA, effectuez l'une des opérations suivantes en fonction de votre shell.

bash shells

Ajoutez la déclaration suivante à `/home/username/.bashrc` et `/home/username/.bash_profile`.

```
export I_MPI_OFI_LIBRARY_INTERNAL=0
```

csch and tcsh shells

Ajoutez la déclaration suivante à `/home/username/.cshrc`.

```
setenv I_MPI_OFI_LIBRARY_INTERNAL 0
```

7. Ajoutez la commande source suivante à votre script shell afin d'extraire le script `vars.sh` du répertoire d'installation pour configurer l'environnement du compilateur à chaque démarrage de l'instance. Effectuez l'une des actions suivantes en fonction de votre shell.

bash shells

Ajoutez la déclaration suivante à `/home/username/.bashrc` et `/home/username/.bash_profile`.

```
source /opt/intel/oneapi/mpi/latest/env/vars.sh
```

csch and tcsh shells

Ajoutez la déclaration suivante à `/home/username/.cshrc`.

```
source /opt/intel/oneapi/mpi/latest/env/vars.csh
```

8. Par défaut, si l'EFA n'est pas disponible en raison d'une mauvaise configuration, Intel MPI utilise par défaut la pile réseau TCP/IP, ce qui peut entraîner un ralentissement des performances des applications. Vous pouvez empêcher cela en définissant `I_MPI_OFI_PROVIDER` sur `efa`. Cela entraîne l'échec d'Intel MPI avec l'erreur suivante si l'EFA n'est pas disponible :

```
Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
error,
MPIR_Init_thread (XXX).....:
MPID_Init (XXXX).....:
MPIDI_OFI_mpi_init_hook (XXXX):
open_fabric (XXXX).....:
find_provider (XXXX).....:
OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
```

Effectuez l'une des actions suivantes en fonction de votre shell.

bash shells

Ajoutez la déclaration suivante à `/home/username/.bashrc` et `/home/username/.bash_profile`.

```
export I_MPI_OFI_PROVIDER=efa
```

csh and tcsh shells

Ajoutez la déclaration suivante à `/home/username/.cshrc`.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. Par défaut, Intel MPI n'imprime pas d'informations de débogage. Vous pouvez spécifier différents niveaux de verbosité pour contrôler les informations de débogage. Les valeurs possibles (dans l'ordre de la quantité de détails qu'elles fournissent) sont : 0 (par défaut), 1, 2, 3, 4, 5. Le niveau 1 et les niveaux supérieurs impriment le résultat de `libfabric version` et de `libfabric provider`. Utilisez `libfabric version` pour vérifier si Intel MPI utilise la bibliothèque Libfabric interne ou celle fournie avec le programme d'installation d'EFA. S'il utilise la bibliothèque Libfabric interne, la version est suffixée par `impi`. Utilisez `libfabric provider` pour vérifier si Intel MPI utilise EFA ou le réseau TCP/IP. S'il utilise EFA, la valeur est `efa`. S'il utilise TCP/IP, la valeur est `tcp;ofi_rxm`.

Pour activer les informations de débogage, effectuez l'une des opérations suivantes en fonction de votre shell.

bash shells

Ajoutez la déclaration suivante à `/home/username/.bashrc` et `/home/username/.bash_profile`.

```
export I_MPI_DEBUG=value
```

csh and tcsh shells

Ajoutez la déclaration suivante à `/home/username/.cshrc`.

```
setenv I_MPI_DEBUG value
```

10. Par défaut, Intel MPI utilise la mémoire partagée du système d'exploitation (shm) pour la communication intra-nœud, et elle utilise Libfabric (ofi) uniquement pour la communication inter-nœuds. En général, cette configuration fournit les meilleures performances. Toutefois, dans certains cas, la structure shm d'Intel MPI peut provoquer le blocage indéfini de certaines applications.

Pour résoudre ce problème, vous pouvez forcer Intel MPI à utiliser Libfabric pour les communications intra-nœud et inter-nœuds. Pour ce faire, effectuez l'une des opérations suivantes en fonction de votre shell.

bash shells

Ajoutez la déclaration suivante à `/home/username/.bashrc` et `/home/username/.bash_profile`.

```
export I_MPI_FABRICS=ofi
```

csh and tcsh shells

Ajoutez la déclaration suivante à `/home/username/.cshrc`.

```
setenv I_MPI_FABRICS ofi
```

Note

Le fournisseur Libfabric d'EFA utilise la mémoire partagée du système d'exploitation pour la communication intra-nœud. Cela signifie que la définition de `I_MPI_FABRICS` sur `ofi` donne des performances similaires à la configuration par défaut `shm:ofi`.

11. Déconnectez-vous de l'instance, puis reconnectez-vous.

Si vous ne souhaitez plus utiliser Intel MPI, supprimez les variables d'environnement des scripts de démarrage de shell.

Étape 6 : Désactiver la protection ptrace

Pour améliorer les performances de votre application HPC, Libfabric utilise la mémoire locale de l'instance pour les communications interprocessus lorsque les processus s'exécutent sur la même instance.

La fonction de mémoire partagée utilise Cross Memory Attach (CMA), non pris en charge avec la protection ptrace. Si vous utilisez une distribution Linux dans laquelle la protection ptrace est activée par défaut, telle que Ubuntu, vous devez la désactiver. Si la protection ptrace n'est pas activée par défaut dans votre distribution Linux, ignorez cette étape.

Pour désactiver la protection ptrace

Effectuez l'une des actions suivantes :

- Pour désactiver temporairement la protection ptrace à des fins de test, exécutez la commande suivante.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Pour désactiver définitivement la protection ptrace, ajoutez `kernel.yama.ptrace_scope = 0` à `/etc/sysctl.d/10-ptrace.conf` et redémarrez l'instance.

Étape 7. Confirmer l'installation

Pour confirmer la réussite de l'installation

1. Pour confirmer que MPI a été installé avec succès, exécutez la commande suivante :

```
$ which mpicc
```

- Pour Open MPI, le chemin renvoyé doit inclure `/opt/amazon/`.
 - Pour Intel MPI, le chemin renvoyé doit inclure `/opt/intel/`. Si vous n'obtenez pas le résultat attendu, assurez-vous d'avoir obtenu le script Intel MPI `vars.sh`.
2. Pour vérifier que les composants du logiciel EFA et Libfabric ont été correctement installés, exécutez la commande suivante.

```
$ C:\> fi_info -p efa -t FI_EP_RDM
```

La commande doit renvoyer des informations sur les interfaces EFA Libfabric. L'exemple suivant illustre la sortie de la commande.

```
provider: efa
  fabric: EFA-fe80::94:3dff:fe89:1b70
  domain: efa_0-rdm
  version: 2.0
  type: FI_EP_RDM
  protocol: FI_PROTO_EFA
```

Étape 8 : Installer votre application HPC

Installez l'application HPC sur l'instance temporaire. La procédure d'installation varie selon l'application HPC. Pour plus d'informations, consultez [Gérer le logiciel sur votre instance AL2](#) dans le guide de l'utilisateur Amazon Linux 2.

Note

Reportez-vous à la documentation de votre application HPC pour obtenir des instructions d'installation.

Étape 9 : Créer une AMI activée pour EFA

Une fois que vous avez installé les composants logiciels requis, vous devez créer une AMI que vous pouvez réutiliser pour lancer vos instances activées pour EFA.

Pour créer une AMI à partir de votre instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée et choisissez Actions, Image, Créer une image.
4. Pour Créer une image, procédez comme suit :
 - a. Pour Nom de l'image, entrez un nom descriptif pour l'AMI.

- b. (Facultatif) Pour Description de l'image, saisissez une brève description de l'objectif de l'AMI.
 - c. Choisissez Create image (Créer une image).
5. Dans le panneau de navigation, sélectionnez AMI.
 6. Recherchez l'AMI que vous avez créée dans la liste. Attendez que le statut passe de pending à available avant de poursuivre avec l'étape suivante.

Étape 10 : Lancer des instances activées pour EFA dans un groupe de placement du cluster

Lancez vos instances activées pour EFA dans un groupe de placement de cluster à l'aide de l'AMI activée pour EFA que vous avez créée à l'Étape 7 et le groupe de sécurité activé pour EFA que vous avez créé à l'Étape 1.

Note

- Vous ne devez pas impérativement lancer vos instances EFA dans un groupe de placement de cluster. Toutefois, nous vous recommandons d'exécuter vos instances activées pour EFA dans un groupe de placement de cluster, car cela lance celles-ci dans un groupe à faible latence au sein d'une zone de disponibilité unique.
- Pour vous assurer que la capacité est disponible lorsque vous mettez à l'échelle les instances de votre cluster, vous pouvez créer une réserve de capacité pour votre groupe de placement du cluster. Pour plus d'informations, consultez [Réerves de capacité dans des groupes de placement de cluster](#).

Pour lancer une instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.
3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que EFA-*instance*. Le nom est attribué à l'instance en tant qu'identification de ressource (Name=*EFA-instance*).

4. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), choisissez My AMIs (Mes AMI), puis sélectionnez l'AMI que vous avez créée à l'étape précédente.
5. Dans la section Instance type (Type d'instance), sélectionnez un [type d'instance pris en charge](#).
6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :
 - a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez pas de sous-réseau, vous ne pouvez pas activer l'instance pour EFA.
 - b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.
 - c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).
8. (Facultatif) Dans la section Storage (Stockage), configurez les volumes selon vos besoins.
9. Dans la section Advanced details (Détails avancés), pour Placement group name (Nom du groupe de placement), sélectionnez le groupe de placement du cluster dans lequel lancer les instances. Si vous avez besoin de créer un groupe de placement du cluster, choisissez Create new placement group (Créer un groupe de placement).
10. Dans le panneau Summary (Récapitulatif) à droite, pour Number of instances (Nombre d'instances), saisissez le nombre d'instances activées pour EFA que vous souhaitez lancer, puis choisissez Launch instance (Lancer l'instance).

Étape 11 : Résilier l'instance temporaire

À ce stade, vous n'avez plus besoin de l'instance temporaire que vous avez lancée. Vous pouvez résilier l'instance pour arrêter d'être facturé pour celle-ci.

Pour résilier l'instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée puis choisissez Actions, État de l'instance, Résilier l'instance.

4. Lorsque vous êtes invité à confirmer, choisissez **Terminate (Mettre fin)**.

Étape 12 : Activer SSH sans mot de passe

Pour permettre à vos applications de s'exécuter sur toutes les instances de votre cluster, vous devez activer l'accès SSH sans mot de passe du nœud principal aux nœuds membres. Le nœud principal est l'instance à partir de laquelle vous exécutez vos applications. Les instances restantes du cluster sont les nœuds membres.

Pour activer SSH sans mot de passe entre les instances du cluster

1. Sélectionnez une instance dans le cluster en tant que nœud principal et connectez-vous à celle-ci.
2. Désactivez `strictHostKeyChecking` et activez `ForwardAgent` sur le nœud principal. Ouvrez le fichier `~/.ssh/config` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Générez une paire de clés RSA

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

La paire de clés est créée dans le répertoire `$HOME/.ssh/`.

4. Modifiez les autorisations de la clé privée sur le nœud principal.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Ouvrez `~/.ssh/id_rsa.pub` à l'aide de l'éditeur de texte de votre choix et copiez la clé.
6. Pour chaque nœud membre du cluster, procédez comme suit :
 - a. Connectez-vous à l'instance.
 - b. Ouvrez `~/.ssh/authorized_keys` à l'aide de l'éditeur de texte de votre choix et ajoutez la clé publique que vous avez copiée plus tôt.

7. Pour tester que le SSH sans mot de passe fonctionne comme prévu, connectez-vous à votre nœud principal et exécutez la commande suivante.

```
$ ssh member_node_private_ip
```

Vous devez vous connecter au nœud membre sans être invité à entrer une clé ou un mot de passe.

Commencer avec EFA et NCCL

La NVIDIA Collective Communications Library (NCCL) est une bibliothèque de routines de communication collectives standard pour plusieurs GPU sur un nœud ou plusieurs nœuds. La NCCL peut être utilisée conjointement avec EFA, Libfabric et MPI pour prendre en charge différentes charges de travail de Machine Learning. Pour plus d'informations, consultez le site web [NCCL](#).

Note

- NCCL avec EFA n'est pris en charge qu'avec des instances p3dn.24xlarge, p4d.24xlarge et p5.48xlarge.
- Seule NCCL 2.4.2 et les versions ultérieures sont prises en charge avec EFA.

Les didacticiels suivants vous permettent de lancer un cluster d'instances EFA et NCCL pour les charges de travail de Machine Learning.

- [Utiliser une AMI de base](#)
- [Utiliser une AMI de AWS Deep Learning](#)

Utiliser une AMI de base

Les étapes suivantes vous permettent de démarrer avec Elastic Fabric Adapter en utilisant une AMI pour l'un des [systèmes d'exploitation de base pris en charge](#).

Note

- Seuls les types d'instance p3dn.24xlarge, p4d.24xlarge et p5.48xlarge sont pris en charge.
- Seules les AMI de base Amazon Linux 2, RHEL 7/8/9, CentOS 7, Rocky Linux 8/9 et Ubuntu 20.04/22.04 sont prises en charge.

Table des matières

- [Étape 1 : Préparer un groupe de sécurité activé pour les EFA](#)
- [Étape 2 : Lancer une instance temporaire](#)
- [Étape 3 : Installer les pilotes GPU Nvidia, le Nvidia CUDA Toolkit et cuDNN](#)
- [Étape 4 : Installer GDRCopy](#)
- [Étape 5 : Installer le logiciel EFA](#)
- [Étape 6 : Installer NCCL](#)
- [Étape 7 : Installation du aws-ofi-nccl plugin](#)
- [Étape 8 : Installer les tests NCCL](#)
- [Étape 9 : Tester votre configuration EFA et NCCL](#)
- [Étape 10 : Installer vos applications de Machine Learning](#)
- [Étape 11 : Créer une AMI activée pour EFA et NCCL](#)
- [Étape 12 : Résilier l'instance temporaire](#)
- [Étape 13 : Lancer les instances activées pour EFA et NCCL dans un groupe de placement du cluster](#)
- [Étape 14 : Activer SSH sans mot de passe](#)

Étape 1 : Préparer un groupe de sécurité activé pour les EFA

Un EFA a besoin d'un groupe de sécurité qui autorise tout le trafic entrant et sortant vers et depuis le groupe de sécurité proprement dit. La procédure suivante crée un groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance de lui-même, et qui autorise le trafic SSH entrant depuis n'importe quelle adresse IPv4 pour la connectivité SSH.

⚠ Important

Ce groupe de sécurité n'est destiné qu'à des fins de test. Pour vos environnements de production, nous vous recommandons de créer une règle SSH entrante qui autorise le trafic uniquement à partir de l'adresse IP à partir de laquelle vous vous connectez, telle que l'adresse IP de votre ordinateur ou une plage d'adresses IP de votre réseau local.

Pour d'autres scénarios, consultez [Règles de groupe de sécurité pour différents cas d'utilisation](#).

Pour créer un groupe de sécurité activé pour EFA

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité), puis Create security group (Créer un groupe de sécurité).
3. Dans la fenêtre Create security group (Créer un groupe de sécurité), procédez comme suit :
 - a. Pour Nom du groupe de sécurité, saisissez un nom descriptif pour le groupe de sécurité, tel que EFA-enabled security group.
 - b. (Facultatif) Pour Description, saisissez une brève description du groupe de sécurité.
 - c. Pour VPC, sélectionnez le VPC dans lequel vous prévoyez de lancer vos instances activées pour EFA.
 - d. Sélectionnez Create security group (Créer un groupe de sécurité).
4. Sélectionnez le groupe de sécurité que vous avez créé et dans l'onglet Details (Détails), copiez le Security group ID (ID du groupe de sécurité).
5. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit inbound rules (Modifier les règles entrantes), puis procédez comme suit :
 - a. Choisissez Ajouter une règle.
 - b. Pour Type, sélectionnez Tout le trafic.
 - c. Pour Source type (Type de source), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.
 - d. Choisissez Ajouter une règle.
 - e. Pour Type, choisissez SSH.
 - f. Pour Source type (Type de source), choisissez Anywhere-IPv4 (IPv4 n'importe où).

- g. Sélectionnez Enregistrer les règles.
6. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit outbound rules (Modifier les règles sortantes), puis procédez comme suit :
 - a. Choisissez Ajouter une règle.
 - b. Pour Type, sélectionnez Tout le trafic.
 - c. Pour Destination type (Type de destination), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.
 - d. Sélectionnez Enregistrer les règles.

Étape 2 : Lancer une instance temporaire

Lancez une instance temporaire que vous pouvez utiliser pour installer et configurer les composants logiciels EFA. Vous utilisez cette instance pour créer une AMI activée pour EFA depuis laquelle vous pouvez lancer vos instances activées pour EFA.

Pour lancer une instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.
3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que EFA-*instance*. Le nom est attribué à l'instance en tant qu'identification de ressource (Name=*EFA-instance*).
4. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez une AMI pour l'un des [systèmes d'exploitation pris en charge](#).
5. Dans la section Type d'instance, sélectionnez p3dn.24xlarge, p4d.24xlarge ou p5.48xlarge.
6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :
 - a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez pas de sous-réseau, vous ne pouvez pas activer l'instance pour EFA.

- b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.
 - c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).
8. Dans la section Storage (Stockage), configurez les volumes selon vos besoins.

 Note

Vous devez provisionner un stockage supplémentaire de 10 à 20 GiB pour le Nvidia CUDA Toolkit. Si vous ne disposez pas d'un espace de stockage suffisant, le message d'erreur `insufficient disk space` s'affichera lors de la tentative d'installation des pilotes Nvidia et de la boîte à outils CUDA.

9. Dans le panneau Summary (Récapitulatif) à droite, choisissez Launch instance (Lancer l'instance).

Étape 3 : Installer les pilotes GPU Nvidia, le Nvidia CUDA Toolkit et cuDNN

Amazon Linux 2

Pour installer les pilotes GPU Nvidia, le Nvidia CUDA Toolkit et cuDNN

1. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance.

```
$ sudo yum upgrade -y && sudo reboot
```

Reconnectez-vous à votre instance après son redémarrage.

2. Installez les utilitaires nécessaires pour l'installation des pilotes GPU Nvidia et du Nvidia CUDA toolkit.

```
$ sudo yum groupinstall 'Development Tools' -y
```

3. Désactiver les nouveaux pilotes Open Source.
 - a. Installez les utilitaires requis et le package d'en-têtes de noyau correspondant à la version du noyau que vous exécutez actuellement.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

- b. Ajoutez nouveau au fichier de liste de refus `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- c. Ajouter `GRUB_CMDLINE_LINUX="rdblacklist=nouveau"` vers le grub fichier et générez à nouveau la configuration Grub.

```
$ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/default/grub \
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Redémarrez l'instance et reconnectez-vous à celle-ci.

5. Préparer les référentiels requis

- a. Installez le référentiel EPEL pour DKMS et activez les référentiels optionnels pour votre distribution Linux.

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- b. Installez la clé GPG publique du référentiel CUDA.

```
$ distribution='rhel7'
```

- c. Configurez le référentiel réseau CUDA et mettez à jour le cache du référentiel.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

- d. (Noyau version 5.10 uniquement) Effectuez ces étapes uniquement si vous utilisez Amazon Linux 2 avec le noyau version 5.10. Si vous utilisez Amazon Linux 2 avec le noyau version 4.12, ignorez ces étapes. Pour vérifier la version de votre noyau, exécutez `uname -r`.
- i. Créez le fichier de configuration du pilote Nvidia nommé `/etc/dkms/nvidia.conf`.

```
$ sudo mkdir -p /etc/dkms \  
&& echo "MAKE[0]=\''make' -j2 module SYSSRC=\${kernel_source_dir}  
IGNORE_XEN_PRESENCE=1 IGNORE_PREEMPT_RT_PRESENCE=1 IGNORE_CC_MISMATCH=1  
CC=/usr/bin/gcc10-gcc\"" | sudo tee /etc/dkms/nvidia.conf
```

- ii. (p4d.24xlarge et p5.48xlarge uniquement) Copiez le fichier de configuration du pilote Nvidia.

```
$ sudo cp /etc/dkms/nvidia.conf /etc/dkms/nvidia-open.conf
```

6. Installer les pilotes GPU Nvidia, la boîte à outils NVIDIA CUDA et cuDNN.

- p3dn.24xlarge

```
$ sudo yum clean all \  
&& sudo yum -y install kmod-nvidia-latest-dkms nvidia-driver-latest-dkms \  
&& sudo yum -y install cuda-drivers-fabricmanager cuda lib cudnn8-devel
```

- p4d.24xlarge et p5.48xlarge

```
$ sudo yum clean all \  
&& sudo yum -y install kmod-nvidia-open-dkms nvidia-driver-latest-dkms \  
&& sudo yum -y install cuda-drivers-fabricmanager cuda lib cudnn8-devel
```

7. Redémarrez l'instance et reconnectez-vous à celle-ci.
8. (p4d.24xlarge et p5.48xlarge uniquement) Démarrez le service Nvidia Fabric Manager et assurez-vous qu'il démarre automatiquement au démarrage de l'instance. Nvidia Fabric Manager est requis pour la gestion des commutateurs NV.

```
$ sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-  
fabricmanager
```

9. Assurez-vous que les chemins d'accès CUDA sont définis chaque fois que l'instance démarre.

- Pour les shells bash , ajoutez les instructions suivantes à `/home/username/.bashrc` et `/home/username/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Pour les shells tcsh , ajoutez les instructions suivantes à `/home/username/.cshrc`.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

10. Pour vérifier que les pilotes GPU Nvidia sont fonctionnels, exécutez la commande suivante.

```
$ nvidia-smi -q | head
```

La commande doit renvoyer des informations sur les GPU Nvidia, les pilotes GPU Nvidia et le Nvidia CUDA Toolkit.

CentOS 7

Pour installer les pilotes GPU Nvidia, le Nvidia CUDA Toolkit et cuDNN

1. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance.

```
$ sudo yum upgrade -y && sudo reboot
```

Reconnectez-vous à votre instance après son redémarrage.

2. Installez les utilitaires nécessaires pour l'installation des pilotes GPU Nvidia et du Nvidia CUDA toolkit.

```
$ sudo yum groupinstall 'Development Tools' -y \
&& sudo yum install -y tar bzip2 make automake pciutils elfutils-libelf-devel
libglvnd-devel iptables firewalld vim bind-utils
```

3. Pour utiliser le pilote GPU Nvidia, vous devez d'abord désactiver les pilotes open source nouveau.

- a. Installez les utilitaires requis et le package d'en-têtes de noyau correspondant à la version du noyau que vous exécutez actuellement.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

- b. Ajoutez nouveau au fichier de liste de refus `/etc/modprobe.d/blacklist.conf`.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- c. Ouvrez le fichier `/etc/default/grub` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- d. Générez à nouveau la configuration Grub.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Redémarrez l'instance et reconnectez-vous à celle-ci.

5. Installer les pilotes GPU Nvidia, la boîte à outils NVIDIA CUDA et cuDNN.

- a. Installez le référentiel EPEL pour DKMS et activez les référentiels optionnels pour votre distribution Linux.

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- b. Installez la clé GPG publique du référentiel CUDA.

```
$ distribution='rhel7'
```

- c. Configurez le référentiel réseau CUDA et mettez à jour le cache du référentiel.

```
$ ARCH=$( /bin/arch ) \  
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/  
compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \  
&& sudo yum clean expire-cache
```

- d. Installez les pilotes NVIDIA, CUDA et cuDNN

```
$ sudo yum clean all \  
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcuda-devel
```

6. Redémarrez l'instance et reconnectez-vous à celle-ci.
7. (p4d.24xlarge et p5.48xlarge uniquement) Démarrez le service Nvidia Fabric Manager et assurez-vous qu'il démarre automatiquement au démarrage de l'instance. Nvidia Fabric Manager est requis pour la gestion des commutateurs NV.

```
$ sudo systemctl start nvidia-fabricmanager \  
&& sudo systemctl enable nvidia-fabricmanager
```

8. Assurez-vous que les chemins d'accès CUDA sont définis chaque fois que l'instance démarre.
 - Pour les shells bash , ajoutez les instructions suivantes à `/home/username/.bashrc` et `/home/username/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH  
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/  
lib64:$LD_LIBRARY_PATH
```

- Pour les shells tcsh , ajoutez les instructions suivantes à `/home/username/.cshrc`.

```
setenv PATH=/usr/local/cuda/bin:$PATH  
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/  
lib64:$LD_LIBRARY_PATH
```

9. Pour vérifier que les pilotes GPU Nvidia sont fonctionnels, exécutez la commande suivante.

```
$ nvidia-smi -q | head
```

La commande doit renvoyer des informations sur les GPU Nvidia, les pilotes GPU Nvidia et le Nvidia CUDA Toolkit.

RHEL 7/8/9 and Rocky Linux 8/9

Pour installer les pilotes GPU Nvidia, le Nvidia CUDA Toolkit et cuDNN

1. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance.

```
$ sudo yum upgrade -y && sudo reboot
```

Reconnectez-vous à votre instance après son redémarrage.

2. Installez les utilitaires nécessaires pour l'installation des pilotes GPU Nvidia et du Nvidia CUDA toolkit.

```
$ sudo yum groupinstall 'Development Tools' -y
```

3. Pour utiliser le pilote GPU Nvidia, vous devez d'abord désactiver les pilotes open source nouveau.
 - a. Installez les utilitaires requis et le package d'en-têtes de noyau correspondant à la version du noyau que vous exécutez actuellement.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

- b. Ajoutez nouveau au fichier de liste de refus `/etc/modprobe.d/blacklist.conf` .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- c. Ouvrez le fichier `/etc/default/grub` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- d. Générez à nouveau la configuration Grub.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Redémarrez l'instance et reconnectez-vous à celle-ci.
5. Installer les pilotes GPU Nvidia, la boîte à outils NVIDIA CUDA et cuDNN.

- a. Installez le référentiel EPEL pour DKMS et activez les référentiels optionnels pour votre distribution Linux.

- RHEL 7

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- RHEL 8 et Rocky Linux 8/9

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

- RHEL 9

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

- b. Installez la clé GPG publique du référentiel CUDA.

```
$ distribution=$(. /etc/os-release;echo $ID`rpm -E "%{?rhel}%{?fedora}"`)
```

- c. Configurez le référentiel réseau CUDA et mettez à jour le cache du référentiel.

```
$ ARCH=$( /bin/arch ) \  
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \  
&& sudo yum clean expire-cache
```

- d. Installez les pilotes NVIDIA, CUDA et cuDNN

```
$ sudo yum clean all \  
$ sudo yum install nvidia-driver-latest-dkms cuda-toolkit-latest-dkms cuda-dkms
```

```
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcuda-devel
```

6. Redémarrez l'instance et reconnectez-vous à celle-ci.
7. (p4d.24xlarge et p5.48xlarge uniquement) Démarrez le service Nvidia Fabric Manager et assurez-vous qu'il démarre automatiquement au démarrage de l'instance. Nvidia Fabric Manager est requis pour la gestion des commutateurs NV.

```
$ sudo systemctl start nvidia-fabricmanager \  
&& sudo systemctl enable nvidia-fabricmanager
```

8. Assurez-vous que les chemins d'accès CUDA sont définis chaque fois que l'instance démarre.
 - Pour les shells bash , ajoutez les instructions suivantes à `/home/username/.bashrc` et `/home/username/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH  
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/  
lib64:$LD_LIBRARY_PATH
```

- Pour les shells tcsh , ajoutez les instructions suivantes à `/home/username/.cshrc`.

```
setenv PATH=/usr/local/cuda/bin:$PATH  
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/  
lib64:$LD_LIBRARY_PATH
```

9. Pour vérifier que les pilotes GPU Nvidia sont fonctionnels, exécutez la commande suivante.

```
$ nvidia-smi -q | head
```

La commande doit renvoyer des informations sur les GPU Nvidia, les pilotes GPU Nvidia et le Nvidia CUDA Toolkit.

Ubuntu 20.04/22.04

Pour installer les pilotes GPU Nvidia, le Nvidia CUDA Toolkit et cuDNN

1. Pour vous assurer que tous vos packages logiciels sont mis à jour, effectuez une mise à jour logicielle rapide sur votre instance.

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

2. Installez les utilitaires nécessaires pour l'installation des pilotes GPU Nvidia et du Nvidia CUDA toolkit.

```
$ sudo apt-get update && sudo apt-get install build-essential -y
```

3. Pour utiliser le pilote GPU Nvidia, vous devez d'abord désactiver les pilotes open source nouveau.

- a. Installez les utilitaires requis et le package d'en-têtes de noyau correspondant à la version du noyau que vous exécutez actuellement.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

- b. Ajoutez nouveau au fichier de liste de refus `/etc/modprobe.d/blacklist.conf`.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- c. Ouvrez le fichier `/etc/default/grub` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- d. Générez à nouveau la configuration Grub.

```
$ sudo update-grub
```

4. Redémarrez l'instance et reconnectez-vous à celle-ci.
5. Ajoutez le référentiel CUDA et installez les pilotes de GPU Nvidia, la boîte à outils NVIDIA CUDA et cuDNN.
 - `p3dn.24xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

- p4d.24xlarge et p5.48xlarge

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-kernel-open-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Redémarrez l'instance et reconnectez-vous à celle-ci.
7. (p4d.24xlarge et p5.48xlarge uniquement) Installez Nvidia Fabric Manager.

- a. Vous devez installer la version de Nvidia Fabric Manager qui correspond à la version du module de noyau Nvidia que vous avez installée à l'étape précédente.

Exécutez la commande suivante pour déterminer la version du module de noyau Nvidia.

```
$ cat /proc/driver/nvidia/version | grep "Kernel Module"
```

Voici un exemple de sortie.

```
NVRM version: NVIDIA UNIX x86_64 Kernel Module 450.42.01 Tue Jun 15
21:26:37 UTC 2021
```

Dans l'exemple ci-dessus, la version principale 450 du module de noyau a été installée. Cela signifie que vous devez installer la version 450 de Nvidia Fabric Manager.

- b. Installez Nvidia Fabric Manager. Exécutez la commande suivante et spécifiez la version principale identifiée à l'étape précédente.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-major_version_number
```

Par exemple, si la version majeure 450 du module de noyau a été installée, utilisez la commande suivante pour installer la version correspondante de Nvidia Fabric Manager.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-450
```

- c. Démarrez le service et assurez-vous qu'il démarre automatiquement au démarrage de l'instance. Nvidia Fabric Manager est requis pour la gestion des commutateurs NV.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Assurez-vous que les chemins d'accès CUDA sont définis chaque fois que l'instance démarre.
 - Pour les shells bash, ajoutez les instructions suivantes à `/home/username/.bashrc` et `/home/username/.bash_profile`.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Pour les shells tcsh , ajoutez les instructions suivantes à `/home/username/.cshrc`.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Pour vérifier que les pilotes GPU Nvidia sont fonctionnels, exécutez la commande suivante.

```
$ nvidia-smi -q | head
```

La commande doit renvoyer des informations sur les GPU Nvidia, les pilotes GPU Nvidia et le Nvidia CUDA Toolkit.

Étape 4 : Installer GDRCopy

Installez GDRCopy pour améliorer les performances de Libfabric. Pour plus d'informations sur GDRCopy, consultez le [référentiel GDRCopy](#) (français non disponible).

Amazon Linux 2, CentOS 7, RHEL 7/8/9, and Rocky Linux 8/9

Pour installer GDRCopy

1. Installez les dépendances obligatoires.

```
$ sudo yum -y install dkms rpm-build make check check-devel subunit subunit-
devel
```

2. Téléchargez et extrayez le package GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz ; cd gdrcopy-2.4/packages
```

3. Créez (build) le package RPM GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Installez le package RPM GDRCopy.

```
$ sudo rpm -Uvh gdrdrv-kmod-2.4-1dkms.noarch*.rpm \  
&& sudo rpm -Uvh gdrdrv-2.4-1.x86_64*.rpm \  
&& sudo rpm -Uvh gdrdrv-devel-2.4-1.noarch*.rpm
```

Ubuntu 20.04/22.04

Pour installer GDRCopy

1. Installez les dépendances obligatoires.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev \  
fakeroot pkg-config dkms
```

2. Téléchargez et extrayez le package GDRCopy.

```
$ wget https://github.com/NVIDIA/gdrdrv/archive/refs/tags/v2.4.tar.gz \  
&& tar xf v2.4.tar.gz \  
&& cd gdrdrv-2.4/packages
```

3. Créez (build) le package RPM GDRCopy.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Installez le package RPM GDRCopy.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \  
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \  
&& sudo dpkg -i gdrdrv-tests_2.4-1_amd64.*.deb \  
&& sudo dpkg -i gdrdrv_2.4-1_amd64.*.deb
```

Étape 5 : Installer le logiciel EFA

Installez le noyau activé pour EFA, les pilotes EFA, Libfabric et la pile Open MPI requis pour prendre en charge EFA sur votre instance temporaire.

Pour installer le logiciel EFA

1. Connectez-vous à l'instance que vous avez lancée. Pour plus d'informations, consultez [Connectez-vous à votre instance Linux](#).
2. Téléchargez les fichiers d'installation du logiciel EFA. Les fichiers d'installation du logiciel sont packagés dans un fichier d'archive compressé (.tar.gz). Pour télécharger la version stable la plus récente, utilisez la commande suivante.

```
$ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz
```

Vous pouvez aussi obtenir la dernière version en remplaçant le numéro de version par `latest` dans la commande ci-dessus.

3. (Facultatif) Vérifiez l'authenticité et l'intégrité du fichier tarball EFA (.tar.gz).

Nous vous recommandons de le faire pour vérifier l'identité de l'éditeur du logiciel et pour vérifier que le fichier n'a pas été modifié ou endommagé depuis sa publication. Si vous ne souhaitez pas vérifier le fichier d'archive, ignorez cette étape.

Note

Sinon, si vous préférez vérifier le fichier d'archive à l'aide d'un total de contrôle MD5 ou SHA256 à la place, consultez [Vérification du programme d'installation EFA à l'aide d'un total de contrôle](#).

- a. Téléchargez la clé publique GPG et importez-la dans votre porte-clés.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --import aws-efa-installer.key
```

La commande doit renvoyer une valeur clé. Notez la valeur clé, car vous en aurez besoin lors de l'étape suivante.

- b. Vérifiez l'empreinte digitale de la clé GPG. Exécutez la commande suivante et spécifiez la valeur clé que vous avez obtenue à l'étape précédente.

```
$ gpg --fingerprint key_value
```

La commande doit renvoyer une empreinte digitale identique à 4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC. Si l'empreinte digitale ne correspond pas, n'exécutez pas le script d'installation EFA et contactez AWS Support.

- c. Téléchargez le fichier SIGNATURE et vérifiez la signature du fichier d'archive EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz.sig
&& gpg --verify ./aws-efa-installer-1.32.0.tar.gz.sig
```

Voici un exemple de sortie.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC
```

Si le résultat inclut `Good signature` et que l'empreinte digitale correspond à l'empreinte digitale renvoyée à l'étape précédente, passez à l'étape suivante. Si ce n'est pas le cas, n'exécutez pas le script d'installation EFA et contactez AWS Support.

4. Procédez à l'extraction des fichiers à partir du fichier compressé `.tar.gz` et accédez au répertoire extrait.

```
$ C:\> tar -xf aws-efa-installer-1.32.0.tar.gz && cd aws-efa-installer
```

5. Exécutez le script d'installation du logiciel EFA.

Note

Depuis EFA 1.30.0, Open MPI 4 et Open MPI 5 sont installés par défaut. À moins que vous n'ayez besoin d'Open MPI 5, nous vous recommandons de n'installer qu'Open MPI 4. La commande suivante installe Open MPI 4 uniquement. Si vous souhaitez installer Open MPI 4 et Open MPI 5, supprimez `--mpi=openmpi4`.

```
$ C:\> sudo ./efa_installer.sh -y --mpi=openmpi4
```

Libfabric est installé dans le répertoire `/opt/amazon/efa`, tandis qu'Open MPI est installé dans le répertoire `/opt/amazon/openmpi`.

- Si le programme d'installation d'EFA vous invite à redémarrer l'instance, faites-le et reconnectez-vous à l'instance. Sinon, déconnectez-vous de l'instance, puis reconnectez-vous pour terminer l'installation.
- Vérifiez que les composants logiciels EFA ont été installés avec succès.

```
$ C:\> fi_info -p efa -t FI_EP_RDM
```

La commande doit renvoyer des informations sur les interfaces EFA Libfabric. L'exemple suivant illustre la sortie de la commande.

- `p3dn.24xlarge` avec interface réseau unique

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` et `p5.48xlarge` avec plusieurs interfaces réseau

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
```

```
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Étape 6 : Installer NCCL

Installez la NCCL. Pour plus d'informations sur la NCCL, consultez le [référentiel NCCL](#).

Pour installer la NCCL.

1. Accédez au répertoire /opt.

```
$ cd /opt
```

2. Clonez le référentiel officiel de la NCCL dans l'instance et accédez au référentiel cloné local.

```
$ sudo git clone https://github.com/NVIDIA/nvml.git && cd nvml
```

3. Créez et installez la NCCL et spécifiez le répertoire d'installation CUDA.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

Étape 7 : Installation du aws-ofi-nccl plugin

Le aws-ofi-nccl plugin fait correspondre les API de transport orientées connexion de NCCL à l'interface fiable sans connexion de Libfabric. Cela vous permet d'utiliser Libfabric comme fournisseur de réseau tout en exécutant des applications basées sur la NCCL. Pour plus d'informations sur le aws-ofi-nccl plugin, consultez le [aws-ofi-nccl référentiel](#).

Pour installer le aws-ofi-nccl plugin

1. Accédez à votre répertoire de base.

```
$ cd $HOME
```

2. (Amazon Linux 2 et Ubuntu uniquement) Installez les utilitaires requis.

- Amazon Linux 2

```
$ sudo yum install hwloc-devel
```

- Ubuntu 20.04

```
$ sudo apt-get install libhwloc-dev
```

3. Téléchargez les fichiers du aws-ofi-nccl plugin. Les fichiers sont packagés dans un fichier d'archive compressé (.tar.gz).

```
$ wget https://github.com/aws/aws-ofi-nccl/releases/download/v1.9.1-aws/aws-ofi-nccl-1.9.1-aws.tar.gz
```

4. Procédez à l'extraction des fichiers à partir du fichier compressé .tar.gz et accédez au répertoire extrait.

```
$ tar -xf aws-ofi-nccl-1.9.1-aws.tar.gz && cd aws-ofi-nccl-1.9.1-aws
```

5. Pour générer les fichiers make, exécutez le script configure et spécifiez les répertoires d'installation MPI, Libfabric, NCCL et CUDA.

```
$ ./configure --prefix=/opt/aws-ofi-nccl --with-mpi=/opt/amazon/openmpi \  
--with-libfabric=/opt/amazon/efa \  
--with-cuda=/usr/local/cuda \  
--enable-platform-aws
```

6. Ajoutez le répertoire Open MPI à la variable PATH.

```
$ export PATH=/opt/amazon/openmpi/bin/:$PATH
```

7. Installez le aws-ofi-nccl plugin.

```
$ make && sudo make install
```

Étape 8 : Installer les tests NCCL

Installez les tests NCCL. Les tests NCCL vous permettent de vous assurer que NCCL a été installée correctement et qu'elle fonctionne normalement. Pour plus d'informations sur les tests NCCL, consultez le [référentiel nccl-tests](#).

Pour installer les tests NCCL

1. Accédez à votre répertoire de base.

```
$ cd $HOME
```

2. Clonez le référentiel officiel nccl-tests dans l'instance et accédez au référentiel cloné local.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Ajoutez le répertoire Libfabric à la variable LD_LIBRARY_PATH.

- Amazon Linux, Amazon Linux 2, RHEL, Rocky Linux 8/9 et CentOS

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
```

- Ubuntu

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
```

4. Installez les tests NCCL et spécifiez les répertoires d'installation MPI, NCCL et CUDA.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/local/cuda
```

Étape 9 : Tester votre configuration EFA et NCCL

Exécutez un test afin de vous assurer que votre instance temporaire est configurée correctement pour EFA et NCCL.

Pour tester votre configuration EFA et NCCL

1. Créez un fichier hôte qui spécifie les hôtes sur lesquels les tests doivent être exécutés. La commande suivante crée un fichier hôte nommé my-hosts qui inclut une référence à l'instance elle-même.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
"X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
meta-data/local-ipv4 >> my-hosts
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
hosts
```

- Exécutez le test et spécifiez le fichier hôte (`--hostfile`) et le nombre de GPU à utiliser (`-n`). La commande suivante exécute le test `all_reduce_perf` sur 8 GPU sur l'instance elle-même et spécifie les variables d'environnement suivantes.
 - `FI_EFA_USE_DEVICE_RDMA=1` : (p4d.24xlarge uniquement) utilise la fonctionnalité RDMA du périphérique pour le transfert unilatéral et bilatéral.
 - `NCCL_DEBUG=INFO` : permet des sorties de débogage détaillées. Vous pouvez également spécifier `VERSION` pour imprimer uniquement la version NCCL au début du test ou `WARN` pour recevoir uniquement des messages d'erreur.

Pour plus d'informations sur les arguments de test NCCL, consultez le [LISEZ-MOI sur les tests NCCL](#) dans le référentiel `nccl-tests` officiel.

- p3dn.24xlarge

```
$ /opt/amazon/openmpi/bin/mpirun \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-
to none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- p4d.24xlarge et p5.48xlarge

```
$ /opt/amazon/openmpi/bin/mpirun \
```

```
-x FI_EFA_USE_DEVICE_RDMA=1 \  
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/  
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \  
-x NCCL_DEBUG=INFO \  
--hostfile my-hosts -n 8 -N 8 \  
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-  
to none \  
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. Vous pouvez confirmer que EFA est actif en tant que fournisseur sous-jacent pour NCCL lorsque le journal NCCL_DEBUG est imprimé.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

Les informations supplémentaires suivantes s'affichent lors de l'utilisation d'une instance p4d.24xlarge.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting  
NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-  
ofi-nccl/xml/p4d-24x1-topo.xml
```

Étape 10 : Installer vos applications de Machine Learning

Installez les applications de machine learning sur l'instance temporaire. La procédure d'installation varie selon l'application de machine learning spécifique. Pour plus d'informations sur l'installation de logiciels sur votre instance Linux, consultez [Gérer les logiciels sur votre instance Amazon Linux 2](#).

Note

Reportez-vous à la documentation de votre application de machine learning pour obtenir des instructions d'installation.

Étape 11 : Créer une AMI activée pour EFA et NCCL

Une fois que vous avez installé les composants logiciels requis, vous devez créer une AMI que vous pouvez réutiliser pour lancer vos instances activées pour EFA.

Pour créer une AMI à partir de votre instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée et choisissez Actions, Image, Créer une image.
4. Pour Créer une image, procédez comme suit :
 - a. Pour Nom de l'image, entrez un nom descriptif pour l'AMI.
 - b. (Facultatif) Pour Description de l'image, saisissez une brève description de l'objectif de l'AMI.
 - c. Choisissez Create image (Créer une image).
5. Dans le panneau de navigation, sélectionnez AMI.
6. Recherchez l'AMI que vous avez créée dans la liste. Attendez que le statut passe de pending à available avant de poursuivre avec l'étape suivante.

Étape 12 : Résilier l'instance temporaire

À ce stade, vous n'avez plus besoin de l'instance temporaire que vous avez lancée. Vous pouvez résilier l'instance pour arrêter d'être facturé pour celle-ci.

Pour résilier l'instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée puis choisissez Actions, État de l'instance, Résilier l'instance.
4. Lorsque vous êtes invité à confirmer, choisissez Terminate (Mettre fin).

Étape 13 : Lancer les instances activées pour EFA et NCCL dans un groupe de placement du cluster

Lancez vos instances activées pour EFA et NCCL dans un groupe de placement du cluster à l'aide de l'AMI activée pour EFA et du groupe de sécurité activé pour EFA que vous avez créés précédemment.

Note

- Vous ne devez pas impérativement lancer vos instances EFA dans un groupe de placement de cluster. Toutefois, nous vous recommandons d'exécuter vos instances activées pour EFA dans un groupe de placement de cluster, car cela lance celles-ci dans un groupe à faible latence au sein d'une zone de disponibilité unique.
- Pour vous assurer que la capacité est disponible lorsque vous mettez à l'échelle les instances de votre cluster, vous pouvez créer une réserve de capacité pour votre groupe de placement du cluster. Pour plus d'informations, consultez [Réerves de capacité dans des groupes de placement de cluster](#).

New console

Pour lancer une instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.
3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que EFA-*instance*. Le nom est attribué à l'instance en tant qu'identification de ressource (Name=*EFA-instance*).
4. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), choisissez My AMIs (Mes AMI), puis sélectionnez l'AMI que vous avez créée à l'étape précédente.
5. Dans la section Instance type (Type d'instance), sélectionnez p3dn.24xlarge ou p4d.24xlarge.
6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :
 - a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez pas de sous-réseau, vous ne pouvez pas activer l'instance pour EFA.

- b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.
 - c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).
8. (Facultatif) Dans la section Storage (Stockage), configurez les volumes selon vos besoins.
9. Dans la section Advanced details (Détails avancés), pour Placement group name (Nom du groupe de placement), sélectionnez le groupe de placement du cluster dans lequel lancer l'instance. Si vous avez besoin de créer un groupe de placement du cluster, choisissez Create new placement group (Créer un groupe de placement).
10. Dans le panneau Summary (Récapitulatif) à droite, pour Number of instances (Nombre d'instances), saisissez le nombre d'instances activées pour EFA que vous souhaitez lancer, puis choisissez Launch instance (Lancer l'instance).

Old console

Pour lancer vos instances activées pour EFA et NCCL dans un groupe de placement du cluster

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Launch Instances.
3. Sur la page Choisir une AMI, choisissez Mes AMI, recherchez l'AMI que vous avez créée précédemment, puis choisissez Sélectionner.
4. Sur la page Choisir un type d'instance, sélectionnez p3dn.24xlarge, puis choisissez Suivant : configurer les détails d'instance.
5. Sur la page Configurer les détails de l'instance, procédez de la façon suivante :
 - a. Pour Nombre d'instances, saisissez le nombre d'instances activées pour EFA et NCCL que vous voulez lancer.
 - b. Pour Réseau et Sous-réseau, sélectionnez le VPC et le sous-réseau dans lesquels lancer les instances.
 - c. Pour le Groupe de placement, sélectionnez Ajoutez une instance au groupe de placement.
 - d. Pour Nom du groupe de placement, sélectionnez Ajouter à un nouveau groupe de placement, puis saisissez un nom descriptif pour le groupe de placement. Ensuite, pour Stratégie du groupe de placement, sélectionnez Cluster.

- e. Pour EFA, choisissez Enable (Activer).
 - f. Dans la section Interfaces réseau, pour l'appareil eth0, choisissez Nouvelle interface réseau. Vous pouvez éventuellement entrer une adresse IPv4 principale et une ou plusieurs adresses IPv4 secondaires. Si vous lancez l'instance dans un sous-réseau auquel un bloc d'adresse CIDR IPv6 est associé, vous pouvez éventuellement spécifier une adresse IPv6 principale et une ou plusieurs adresses IPv6 secondaires.
 - g. Choisissez Suivant : Ajouter un stockage.
6. Sur la page Ajouter un stockage, spécifiez les volumes à attacher aux instances, outre ceux spécifiés par l'AMI (par exemple, le volume du périphérique racine). Choisissez ensuite Suivant : Ajouter des balises.
 7. Sur la page Ajouter des balises, spécifiez des balises pour l'instance, par exemple un nom évocateur, puis sélectionnez Suivant : Configurer le groupe de sécurité.
 8. Sur la page Configurer le groupe de sécurité, cliquez sur Attribuer un groupe de sécurité, choisissez Sélectionner un groupe de sécurité existant, puis le groupe de sécurité que vous avez créé précédemment.
 9. Choisissez Vérifier et lancer.
 10. Sur la page Examiner le lancement de l'instance, vérifiez les paramètres, puis choisissez Lancer pour sélectionner une paire de clés et lancer votre instance.

Étape 14 : Activer SSH sans mot de passe

Pour permettre à vos applications de s'exécuter sur toutes les instances de votre cluster, vous devez activer l'accès SSH sans mot de passe du nœud principal aux nœuds membres. Le nœud principal est l'instance à partir de laquelle vous exécutez vos applications. Les instances restantes du cluster sont les nœuds membres.

Pour activer SSH sans mot de passe entre les instances du cluster

1. Sélectionnez une instance dans le cluster en tant que nœud principal et connectez-vous à celle-ci.
2. Désactivez `strictHostKeyChecking` et activez `ForwardAgent` sur le nœud principal. Ouvrez le fichier `~/.ssh/config` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
Host *  
    ForwardAgent yes
```

```
Host *
    StrictHostKeyChecking no
```

3. Générez une paire de clés RSA

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

La paire de clés est créée dans le répertoire `$HOME/.ssh/`.

4. Modifiez les autorisations de la clé privée sur le nœud principal.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Ouvrez `~/.ssh/id_rsa.pub` à l'aide de l'éditeur de texte de votre choix et copiez la clé.

6. Pour chaque nœud membre du cluster, procédez comme suit :

- a. Connectez-vous à l'instance.
- b. Ouvrez `~/.ssh/authorized_keys` à l'aide de l'éditeur de texte de votre choix et ajoutez la clé publique que vous avez copiée plus tôt.

7. Pour tester que le SSH sans mot de passe fonctionne comme prévu, connectez-vous à votre nœud principal et exécutez la commande suivante.

```
$ ssh member_node_private_ip
```

Vous devez vous connecter au nœud membre sans être invité à entrer une clé ou un mot de passe.

Utiliser une AMI de AWS Deep Learning

Les étapes suivantes vous aideront à démarrer avec l'une des AMI de AWS Deep Learning suivantes :

- AMI de deep learning (Amazon Linux 2)
- AMI de deep learning (Ubuntu 20.04)

Pour de plus amples informations, consultez le [AWS Deep Learning AMI Guide de l'utilisateur](#).

 Note

Seuls les types d'instance p3dn.24xlarge et p4d.24xlarge sont pris en charge.

Sommaire

- [Étape 1 : Préparer un groupe de sécurité activé pour les EFA](#)
- [Étape 2 : Lancer une instance temporaire](#)
- [Étape 3 : Tester votre configuration EFA et NCCL](#)
- [Étape 4 : Installer vos applications de Machine Learning](#)
- [Étape 5 : Créer une AMI activée pour EFA et NCCL](#)
- [Étape 6 : Résilier l'instance temporaire](#)
- [Étape 7 : Lancer les instances activées pour EFA et NCCL dans un groupe de placement de cluster](#)
- [Étape 8 : Activer SSH sans mot de passe](#)

Étape 1 : Préparer un groupe de sécurité activé pour les EFA

Un EFA a besoin d'un groupe de sécurité qui autorise tout le trafic entrant et sortant vers et depuis le groupe de sécurité proprement dit. La procédure suivante crée un groupe de sécurité qui autorise tout le trafic entrant et sortant à destination et en provenance de lui-même, et qui autorise le trafic SSH entrant depuis n'importe quelle adresse IPv4 pour la connectivité SSH.

 Important

Ce groupe de sécurité n'est destiné qu'à des fins de test. Pour vos environnements de production, nous vous recommandons de créer une règle SSH entrante qui autorise le trafic uniquement à partir de l'adresse IP à partir de laquelle vous vous connectez, telle que l'adresse IP de votre ordinateur ou une plage d'adresses IP de votre réseau local.

Pour d'autres scénarios, consultez [Règles de groupe de sécurité pour différents cas d'utilisation](#).

Pour créer un groupe de sécurité activé pour EFA

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, choisissez Security Groups (Groupes de sécurité), puis Create security group (Créer un groupe de sécurité).
3. Dans la fenêtre Create security group (Créer un groupe de sécurité), procédez comme suit :
 - a. Pour Nom du groupe de sécurité, saisissez un nom descriptif pour le groupe de sécurité, tel que `EFA-enabled security group`.
 - b. (Facultatif) Pour Description, saisissez une brève description du groupe de sécurité.
 - c. Pour VPC, sélectionnez le VPC dans lequel vous prévoyez de lancer vos instances activées pour EFA.
 - d. Sélectionnez Create security group (Créer un groupe de sécurité).
4. Sélectionnez le groupe de sécurité que vous avez créé et dans l'onglet Details (Détails), copiez le Security group ID (ID du groupe de sécurité).
5. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit inbound rules (Modifier les règles entrantes), puis procédez comme suit :
 - a. Choisissez Ajouter une règle.
 - b. Pour Type, sélectionnez Tout le trafic.
 - c. Pour Source type (Type de source), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.
 - d. Choisissez Ajouter une règle.
 - e. Pour Type, choisissez SSH.
 - f. Pour Source type (Type de source), choisissez Anywhere-IPv4 (IPv4 n'importe où).
 - g. Sélectionnez Enregistrer les règles.
6. En conservant la sélection du groupe de sécurité, choisissez Actions, Edit outbound rules (Modifier les règles sortantes), puis procédez comme suit :
 - a. Choisissez Ajouter une règle.
 - b. Pour Type, sélectionnez Tout le trafic.
 - c. Pour Destination type (Type de destination), choisissez Custom (Personnalisée) et collez l'ID du groupe de sécurité que vous avez copié dans le champ.
 - d. Sélectionnez Enregistrer les règles.

Étape 2 : Lancer une instance temporaire

Lancez une instance temporaire que vous pouvez utiliser pour installer et configurer les composants logiciels EFA. Vous utilisez cette instance pour créer une AMI activée pour EFA depuis laquelle vous pouvez lancer vos instances activées pour EFA.

Pour lancer une instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.
3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que EFA-*instance*. Le nom est attribué à l'instance en tant qu'identification de ressource (Name=*EFA-instance*).
4. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez une AMI AWS Deep Learning version 25.0 ou ultérieure prise en charge.
5. Dans la section Instance type (Type d'instance), sélectionnez p3dn.24xlarge ou p4d.24xlarge.
6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :
 - a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez pas de sous-réseau, vous ne pouvez pas activer l'instance pour EFA.
 - b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.
 - c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).
8. Dans la section Storage (Stockage), configurez les volumes selon vos besoins.

Note

Vous devez provisionner un stockage supplémentaire de 10 à 20 GiB pour le Nvidia CUDA Toolkit. Si vous ne disposez pas d'un espace de stockage suffisant, le message

d'erreur `insufficient disk space` s'affichera lors de la tentative d'installation des pilotes Nvidia et de la boîte à outils CUDA.

9. Dans le panneau Summary (Récapitulatif) à droite, choisissez Launch instance (Lancer l'instance).

Étape 3 : Tester votre configuration EFA et NCCL

Exécutez un test afin de vous assurer que votre instance temporaire est configurée correctement pour EFA et NCCL.

Pour tester votre configuration EFA et NCCL

1. Créez un fichier hôte qui spécifie les hôtes sur lesquels les tests doivent être exécutés. La commande suivante crée un fichier hôte nommé `my-hosts` qui inclut une référence à l'instance elle-même.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/local-ipv4 >> my-hosts
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-hosts
```

2. Exécutez le test et spécifiez le fichier hôte (`--hostfile`) et le nombre de GPU à utiliser (`-n`). La commande suivante exécute le test `all_reduce_perf` sur 8 GPU sur l'instance elle-même et spécifie les variables d'environnement suivantes.
 - `FI_EFA_USE_DEVICE_RDMA=1` : (p4d.24xlarge uniquement) utilise la fonctionnalité RDMA du périphérique pour le transfert unilatéral et bilatéral.
 - `NCCL_DEBUG=INFO` : permet des sorties de débogage détaillées. Vous pouvez également spécifier `VERSION` pour imprimer uniquement la version NCCL au début du test ou `WARN` pour recevoir uniquement des messages d'erreur.

Pour plus d'informations sur les arguments de test NCCL, consultez le [LISEZ-MOI sur les tests NCCL](#) dans le référentiel nccl-tests officiel.

- p3dn.24xlarge

```
$ /opt/amazon/openmpi/bin/mpirun \  
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/  
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \  
-x NCCL_DEBUG=INFO \  
--hostfile my-hosts -n 8 -N 8 \  
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-  
to none \  
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- p4d.24xlarge

```
$ /opt/amazon/openmpi/bin/mpirun \  
-x FI_EFA_USE_DEVICE_RDMA=1 \  
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/  
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \  
-x NCCL_DEBUG=INFO \  
--hostfile my-hosts -n 8 -N 8 \  
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-  
to none \  
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. Vous pouvez confirmer que EFA est actif en tant que fournisseur sous-jacent pour NCCL lorsque le journal NCCL_DEBUG est imprimé.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

Les informations supplémentaires suivantes s'affichent lors de l'utilisation d'une instance p4d.24xlarge.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting  
NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-  
ofi-nccl/xml/p4d-24x1-topo.xml
```

Étape 4 : Installer vos applications de Machine Learning

Installez les applications de machine learning sur l'instance temporaire. La procédure d'installation varie selon l'application de machine learning spécifique. Pour plus d'informations sur l'installation de logiciels sur votre instance Linux, consultez [Gérer les logiciels sur votre instance Amazon Linux 2](#).

Note

Reportez-vous à la documentation de votre application de machine learning pour obtenir des instructions d'installation.

Étape 5 : Créer une AMI activée pour EFA et NCCL

Une fois que vous avez installé les composants logiciels requis, vous devez créer une AMI que vous pouvez réutiliser pour lancer vos instances activées pour EFA.

Pour créer une AMI à partir de votre instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée et choisissez Actions, Image, Créer une image.
4. Pour Créer une image, procédez comme suit :
 - a. Pour Nom de l'image, entrez un nom descriptif pour l'AMI.
 - b. (Facultatif) Pour Description de l'image, saisissez une brève description de l'objectif de l'AMI.
 - c. Choisissez Create image (Créer une image).
5. Dans le panneau de navigation, sélectionnez AMI.
6. Recherchez l'AMI que vous avez créée dans la liste. Attendez que le statut passe de pending à available avant de poursuivre avec l'étape suivante.

Étape 6 : Résilier l'instance temporaire

À ce stade, vous n'avez plus besoin de l'instance temporaire que vous avez lancée. Vous pouvez résilier l'instance pour arrêter d'être facturé pour celle-ci.

Pour résilier l'instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance temporaire que vous avez créée puis choisissez Actions, État de l'instance, Résilier l'instance.
4. Lorsque vous êtes invité à confirmer, choisissez Terminate (Mettre fin).

Étape 7 : Lancer les instances activées pour EFA et NCCL dans un groupe de placement de cluster

Lancez vos instances activées pour EFA et NCCL dans un groupe de placement du cluster à l'aide de l'AMI activée pour EFA et du groupe de sécurité activé pour EFA que vous avez créés précédemment.

Note

- Vous ne devez pas impérativement lancer vos instances EFA dans un groupe de placement de cluster. Toutefois, nous vous recommandons d'exécuter vos instances activées pour EFA dans un groupe de placement de cluster, car cela lance celles-ci dans un groupe à faible latence au sein d'une zone de disponibilité unique.
- Pour vous assurer que la capacité est disponible lorsque vous mettez à l'échelle les instances de votre cluster, vous pouvez créer une réserve de capacité pour votre groupe de placement du cluster. Pour plus d'informations, consultez [Réerves de capacité dans des groupes de placement de cluster](#).

New console

Pour lancer une instance temporaire

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances, puis Launch Instances (Lancer des instances) pour ouvrir le nouvel assistant de lancement d'instance.
3. (Facultatif) Dans la section Name and tags (Noms et identifications), fournissez un nom pour l'instance, tel que EFA-*instance*. Le nom est attribué à l'instance en tant qu'identification de ressource (Name=*EFA-instance*).

4. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), choisissez My AMIs (Mes AMI), puis sélectionnez l'AMI que vous avez créée à l'étape précédente.
5. Dans la section Instance type (Type d'instance), sélectionnez p3dn.24xlarge ou p4d.24xlarge.
6. Dans la section Key pair (Paire de clés), sélectionnez la paire de clés à utiliser pour l'instance.
7. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis procédez comme suit :
 - a. Pour Sous-réseau, choisissez le sous-réseau dans lequel lancer l'instance. Si vous ne sélectionnez pas de sous-réseau, vous ne pouvez pas activer l'instance pour EFA.
 - b. Pour Firewall (security groups) (Pare-feu (groupes de sécurité)), choisissez Sélectionner un groupe de sécurité existant (Select existing security group), puis sélectionnez le groupe de sécurité que vous avez créé à l'étape précédente.
 - c. Développez la section Advanced network configuration (Configuration réseau avancée) et pour Elastic Fabric Adapter (EFA), sélectionnez Enable (Activer).
8. (Facultatif) Dans la section Storage (Stockage), configurez les volumes selon vos besoins.
9. Dans la section Advanced details (Détails avancés), pour Placement group name (Nom du groupe de placement), sélectionnez le groupe de placement du cluster dans lequel lancer l'instance. Si vous avez besoin de créer un groupe de placement du cluster, choisissez Create new placement group (Créer un groupe de placement).
10. Dans le panneau Summary (Récapitulatif) à droite, pour Number of instances (Nombre d'instances), saisissez le nombre d'instances activées pour EFA que vous souhaitez lancer, puis choisissez Launch instance (Lancer l'instance).

Old console

Pour lancer vos instances activées pour EFA et NCCL dans un groupe de placement du cluster

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Launch Instances.
3. Sur la page Choisir une AMI, choisissez Mes AMI, recherchez l'AMI que vous avez créée précédemment, puis choisissez Sélectionner.

4. Sur la page Choisir un type d'instance, sélectionnez p3dn.24xlarge, puis choisissez Suivant : configurer les détails d'instance.
5. Sur la page Configurer les détails de l'instance, procédez de la façon suivante :
 - a. Pour Nombre d'instances, saisissez le nombre d'instances activées pour EFA et NCCL que vous voulez lancer.
 - b. Pour Réseau et Sous-réseau, sélectionnez le VPC et le sous-réseau dans lesquels lancer les instances.
 - c. Pour le Groupe de placement, sélectionnez Ajoutez une instance au groupe de placement.
 - d. Pour Nom du groupe de placement, sélectionnez Ajouter à un nouveau groupe de placement, puis saisissez un nom descriptif pour le groupe de placement. Ensuite, pour Stratégie du groupe de placement, sélectionnez Cluster.
 - e. Pour EFA, choisissez Enable (Activer).
 - f. Dans la section Interfaces réseau, pour l'appareil eth0, choisissez Nouvelle interface réseau. Vous pouvez éventuellement entrer une adresse IPv4 principale et une ou plusieurs adresses IPv4 secondaires. Si vous lancez l'instance dans un sous-réseau auquel un bloc d'adresse CIDR IPv6 est associé, vous pouvez éventuellement spécifier une adresse IPv6 principale et une ou plusieurs adresses IPv6 secondaires.
 - g. Choisissez Suivant : Ajouter un stockage.
6. Sur la page Ajouter un stockage, spécifiez les volumes à attacher aux instances, outre ceux spécifiés par l'AMI (par exemple, le volume du périphérique racine). Choisissez ensuite Suivant : Ajouter des balises.
7. Sur la page Ajouter des balises, spécifiez des balises pour l'instance, par exemple un nom évocateur, puis sélectionnez Suivant : Configurer le groupe de sécurité.
8. Sur la page Configurer le groupe de sécurité, cliquez sur Attribuer un groupe de sécurité, choisissez Sélectionner un groupe de sécurité existant, puis le groupe de sécurité que vous avez créé précédemment.
9. Choisissez Vérifier et lancer.
10. Sur la page Examiner le lancement de l'instance, vérifiez les paramètres, puis choisissez Lancer pour sélectionner une paire de clés et lancer votre instance.

Étape 8 : Activer SSH sans mot de passe

Pour permettre à vos applications de s'exécuter sur toutes les instances de votre cluster, vous devez activer l'accès SSH sans mot de passe du nœud principal aux nœuds membres. Le nœud principal est l'instance à partir de laquelle vous exécutez vos applications. Les instances restantes du cluster sont les nœuds membres.

Pour activer SSH sans mot de passe entre les instances du cluster

1. Sélectionnez une instance dans le cluster en tant que nœud principal et connectez-vous à celle-ci.
2. Désactivez `strictHostKeyChecking` et activez `ForwardAgent` sur le nœud principal. Ouvrez le fichier `~/.ssh/config` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Générez une paire de clés RSA

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

La paire de clés est créée dans le répertoire `$HOME/.ssh/`.

4. Modifiez les autorisations de la clé privée sur le nœud principal.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Ouvrez `~/.ssh/id_rsa.pub` à l'aide de l'éditeur de texte de votre choix et copiez la clé.
6. Pour chaque nœud membre du cluster, procédez comme suit :
 - a. Connectez-vous à l'instance.
 - b. Ouvrez `~/.ssh/authorized_keys` à l'aide de l'éditeur de texte de votre choix et ajoutez la clé publique que vous avez copiée plus tôt.
7. Pour tester que le SSH sans mot de passe fonctionne comme prévu, connectez-vous à votre nœud principal et exécutez la commande suivante.

```
$ ssh member_node_private_ip
```

Vous devez vous connecter au nœud membre sans être invité à entrer une clé ou un mot de passe.

Travailler avec EFA

Vous pouvez créer, utiliser et gérer un EFA tout comme n'importe quelle interface réseau Elastic dans Amazon EC2. En revanche, contrairement aux interfaces réseau Elastic, les EFAs ne peuvent pas être attachés à une instance ou détachés de celle-ci à l'état d'exécution.

Exigences relatives à EFA

Pour utiliser EFA, vous devez procéder comme suit :

- Choisissez l'un des [types d'instance pris en charge](#).
- Utilisez une AMI pour l'un des [systèmes d'exploitation pris en charge](#).
- Installez les composants logiciels EFA. Pour plus d'informations, consultez [Étape 3 : Installer le logiciel EFA](#) et [Étape 5 : \(Facultatif\) Installer Intel MPI](#).
- Utilisez un groupe de sécurité qui autorise tout le trafic entrant et sortant vers et depuis le groupe de sécurité proprement dit. Pour plus d'informations, consultez [Étape 1 : Préparer un groupe de sécurité activé pour les EFA](#).

Sommaire

- [Créer un EFA](#)
- [Attacher un EFA à une instance arrêtée](#)
- [Attacher un EFA lors du lancement d'une instance](#)
- [Ajouter un EFA à un modèle de lancement](#)
- [Gérer les adresses IP d'un EFA](#)
- [Modifier le groupe de sécurité d'un EFA](#)
- [Détacher un EFA](#)
- [Afficher un EFAs](#)
- [Supprimer un EFA](#)

Créer un EFA

Vous pouvez créer un EFA dans un sous-réseau au sein d'un VPC. Vous ne pouvez pas déplacer l'EFA vers un autre sous-réseau une fois qu'il a été créé et vous pouvez uniquement l'attacher à des instances arrêtées dans la même zone de disponibilité.

Pour créer un(e) EFA à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces.
3. Sélectionnez Créer une interface réseau.
4. Pour Description, saisissez un nom descriptif pour l'EFA.
5. Pour Sous-réseau, sélectionnez le sous-réseau dans lequel créer l'EFA.
6. Pour IP privée, saisissez l'adresse IPv4 privée principale. Si vous ne spécifiez pas d'adresse IPv4, nous sélectionnons une adresse IPv4 privée disponible dans le sous-réseau sélectionné.
7. (IPv6 uniquement) Si vous avez sélectionné un sous-réseau qui a un bloc d'adresse CIDR IPv6 associé, vous pouvez le cas échéant spécifier une adresse IPv6 dans le champ IP IPv6.
8. Pour Groupes de sécurité, sélectionnez un ou plusieurs groupes de sécurité.
9. Pour EFA, choisissez Activé.
10. Choisissez Yes, Create.

Pour créer un nouvel EFA à l'aide du AWS CLI

Utilisez la commande [create-network-interface](#) et pour `interface-type`, spécifiez `efa`, comme dans l'exemple suivant.

```
aws ec2 create-network-interface --subnet-id subnet-01234567890 --  
description example_efa --interface-type efa
```

Attacher un EFA à une instance arrêtée

Vous pouvez attacher un EFA à toute instance prise en charge à l'état `stopped`. Vous ne pouvez pas attacher un EFA à une instance à l'état `running`. Pour plus d'informations sur les types d'instance pris en charge, consultez [Types d'instance pris en charge](#).

Vous attachez un EFA à une instance de la même manière que vous attachez une interface réseau à une instance. Pour plus d'informations, consultez [Attacher une interface réseau à une instance](#).

Attacher un EFA lors du lancement d'une instance

Pour attacher un EFA existant lors du lancement d'une instance (AWS CLI)

Utilisez la commande [run-instances](#) et pour NetworkInterfaceId, spécifiez l'ID de l'EFA, comme indiqué dans l'exemple suivant.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-type c5n.18xlarge --key-name my_key_pair --network-interfaces DeviceIndex=0,NetworkInterfaceId=efa_id,Groups=sg_id,SubnetId=subnet_id
```

Pour attacher un nouvel EFA lors du lancement d'une instance (AWS CLI)

Utilisez la commande [run-instances](#) et pour InterfaceType, spécifiez `efa`, comme indiqué dans l'exemple suivant.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-type c5n.18xlarge --key-name my_key_pair --network-interfaces DeviceIndex=0,InterfaceType=efa,Groups=sg_id,SubnetId=subnet_id
```

Ajouter un EFA à un modèle de lancement

Vous pouvez créer un modèle de lancement contenant les informations de configuration nécessaires pour lancer des instances activées pour EFA. Pour créer un modèle de lancement activé pour EFA, créez un nouveau modèle de lancement, et spécifiez un type d'instance pris en charge, votre AMI activée pour EFA et un groupe de sécurité activé pour EFA. Pour plus d'informations, consultez [Commencer avec EFA et MPI](#).

Vous pouvez tirer parti des modèles de lancement pour lancer des instances activées pour EFA avec d'autres services AWS comme [AWS Batch](#) ou [AWS ParallelCluster](#).

Pour plus d'informations sur la création de modèles de lancement, consultez [Création d'un modèle de lancement](#).

Gérer les adresses IP d'un EFA

Vous pouvez modifier les adresses IP associées à un EFA. Si vous avez une adresse IP Elastic, vous pouvez l'associer à un EFA. Si votre EFA est mis en service dans un sous-réseau auquel un bloc d'adresses CIDR IPv6 est associé, vous pouvez attribuer une ou plusieurs adresses IPv6 à l'EFA.

Vous attribuez des adresses IP Elastic (IPv4) et IPv6 à un EFA tout comme vous attribuez une adresse IP à une interface réseau Elastic. Pour plus d'informations, consultez [Gestion des adresses IP](#).

Modifier le groupe de sécurité d'un EFA

Vous pouvez modifier le groupe de sécurité associé à un EFA. Pour que vous puissiez activer la fonctionnalité de contournement du système d'exploitation, l'EFA doit appartenir à un groupe de sécurité qui autorise tout le trafic entrant et sortant vers et depuis le groupe de sécurité proprement dit.

Vous pouvez modifier le groupe de sécurité associé à un EFA comme vous le feriez pour un groupe de sécurité associé à une interface réseau Elastic. Pour plus d'informations, consultez [Modification du groupe de sécurité](#).

Détacher un EFA

Pour détacher un EFA d'une instance, vous devez d'abord arrêter l'instance. Vous ne pouvez pas détacher un EFA d'une instance à l'état d'exécution.

Vous détachez un EFA d'une instance tout comme vous détachez une interface réseau Elastic d'une instance. Pour plus d'informations, consultez [Détacher une interface réseau d'une instance](#).

Afficher un EFAs

Vous pouvez afficher tous les EFAs de votre compte.

Vous affichez les EFAs comme vous le feriez pour les interfaces réseau Elastic. Pour plus d'informations, consultez [Afficher les détails relatifs à une interface réseau](#).

Supprimer un EFA

Pour supprimer un EFA, vous devez d'abord le détacher de l'instance. Vous ne pouvez pas supprimer un EFA pendant qu'il est attaché à une instance.

Vous supprimez les EFAs comme vous le feriez pour les interfaces réseau Elastic. Pour plus d'informations, consultez [Supprimer une interface réseau](#).

Surveillez un EFA

Vous pouvez utiliser les fonctions suivantes pour surveiller les performances de vos Elastic Fabric Adapters.

Journaux de flux Amazon VPC

Vous pouvez créer un journal de flux Amazon VPC pour capturer des informations sur le trafic entrant ou sortant de votre EFA. Les données des journaux de flux peuvent être publiées sur Amazon CloudWatch Logs et Amazon S3. Une fois que vous avez créé un journal de flux, vous pouvez extraire et afficher ses données dans la destination choisie. Pour plus d'informations, consultez [Journaux de flux VPC](#) dans le Amazon VPC Guide de l'utilisateur.

Vous créez un journal de flux pour un EFA comme vous le feriez pour une interface réseau Elastic. Pour plus d'informations, consultez [Créer un journal de flux](#) dans le Guide de l'utilisateur Amazon VPC.

Dans les entrées de journal de flux, le trafic EFA est identifié par des adresses `srcAddress` et `destAddress`, qui sont formatées comme des adresses MAC, comme dans l'exemple suivant.

version	accountId	eniId	srcAddress		destAddress		sourcePort	destPort
protocol	packets	bytes	start	end	action	log-status		
2	3794735123	eni-10000001	01:23:45:67:89:ab	05:23:45:67:89:ab	-	-	-	-
-	9	5689	1521232534	1524512343	ACCEPT	OK		

Amazon CloudWatch

Amazon CloudWatch fournit des statistiques qui vous permettent de surveiller vos EFA en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Pour plus d'informations, consultez [Surveillez vos instances à l'aide de CloudWatch](#).

Vérification du programme d'installation EFA à l'aide d'un total de contrôle

Vous pouvez éventuellement vérifier l'archive EFA (fichier .tar.gz) à l'aide d'un total de contrôle MD5 ou SHA256. Nous vous recommandons de le faire pour vérifier l'identité de l'éditeur du logiciel et pour vérifier que l'application n'a pas été modifiée ou endommagée depuis sa publication.

Pour vérifier l'archive

Utilisez l'utilitaire md5sum pour le total de contrôle MD5 ou l'utilitaire sha256sum pour le total de contrôle SHA256 et spécifiez le nom du fichier tarball. Vous devez exécuter la commande à partir du répertoire dans lequel vous avez enregistré le fichier tarball.

- MD5

```
$ md5sum tarball_filename.tar.gz
```

- SHA256

```
$ sha256sum tarball_filename.tar.gz
```

Les commandes doivent renvoyer une valeur du total de contrôle au format suivant.

```
checksum_value tarball_filename.tar.gz
```

Comparez la valeur du total de contrôle renvoyée par la commande avec la valeur du total de contrôle fournie dans le tableau ci-dessous. Si les totaux de contrôle correspondent, on peut alors exécuter le script d'installation en toute sécurité. Si les totaux de contrôle ne correspondent pas, n'exécutez pas le script d'installation et contactez AWS Support.

Par exemple, la commande suivante vérifie l'archive EFA 1.9.4 à l'aide du total de contrôle SHA256.

```
$ sha256sum aws-efa-installer-1.9.4.tar.gz
```

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-  
installer-1.9.4.tar.gz
```

Le tableau suivant répertorie les totaux de contrôle des versions récentes de EFA.

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1.32.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.32.0.tar.gz	MD5: db8d65cc028d8d08b5 a9f2d88881c1b1 SHA256: 5f7233760be57f6fee 6de8c09acbfbf59238 de848e06048dc54d15 6ef578fc66
EFA 1.31.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.31.0.tar.gz	MD5: 856352f12bef2ccbad cd75e35aa52aaf SHA256: 943325bd37902a4300 ac9e5715163537d56e cb4e7b87b37827c3e5 47aa1897bf
EFA 1,30.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.30.0.tar.gz	MD5: 31f48e1a47fe93ede8 ebd273fb747358 SHA256: 876ab9403e07a0c3c9 1a1a34685a52eced89 0ae052df94857f6081 c5f6c78a0a
EFA 1.29.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.29.1.tar.gz	MD5: e1872ca815d752c1d7 c2b5c175e52a16 SHA256: 178b263b8c25845b63 dc93b25bcdff5870df 5204ec509af26f43e8 d283488744
EFA 1.29.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.29.0.tar.gz	MD5: 39d06a002154d94cd9 82ed348133f385 SHA256: 836655f87015547e73 3e7d9f7c760e4e2469

Version	Télécharger le kit URL	Totaux de contrôle
		7f8bbc261bb5f3560a bd4206bc36
EFA 1.28.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.28.0.tar.gz	MD5: 9dc13b744666582260 5e66febe074035 SHA256: 2e625d2d6d3e073b51 78e8e861891273d896 b66d03cb1a32244fd5 6789f1c435
EFA 1.27.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.27.0.tar.gz	MD5: 98bfb515ea3e8d93f5 54020f3837fa15 SHA256: 1d49a97b0bf8d964d9 1652a79ac851f2550e 33a5bf9d0cf86ec935 7ff6579aa3
EFA 1.26.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.26.1.tar.gz	MD5: 884e74671fdef47255 01f7cd2d451d0c SHA256: c616994c924f54ebfa bfab32b7fe8ac56947 fae00a0ff453d975e2 98d174fc96
EFA 1.26.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.26.0.tar.gz	MD5: f8839f12ff2e3b9ba0 9ae8a82b30e663 SHA256: bc1abc1f76e97d204d 3755d2a9ca307fc423 e51c63141f798c2f15 be3715aa11

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1,25.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.25.1.tar.gz	MD5: 6d876b894547847a45 bb8854d4431f18 SHA256: d2abc553d22b89a4ce 92882052c1fa6de450 d3a801fe005da718b7 d4b9602b06
EFA 1.25.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.25.0.tar.gz	MD5: 1993836ca749596051 da04694ea0d00c SHA256: 98b7b26ce031a2d6a9 3de2297cc71b03af64 7194866369ca53b60d 82d45ad342
EFA 1.24.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.24.1.tar.gz	MD5: 211b249f39d53086f3 cb0c07665f4e6f SHA256: 120cfeec233af09556 23ac7133b674143329 f9561a9a8193e47306 0f596aec62
EFA 1.24.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.24.0.tar.gz	MD5: 7afe0187951e2dd2c9 cc4b572e62f924 SHA256: 878623f819a0d9099d 76ecd41cf4f569d4c3 aac0c9bb7ba9536347 c50b6bf88e

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1.23.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.23.1.tar.gz	MD5: 22491e114b6ee7160a 8290145dca0c28 SHA256: 5ca848d8e0ff4d1571 cd443c36f8d27c8cdf 2a0c97e9068ebf000c 303fc40797
EFA 1.23.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.23.0.tar.gz	MD5: 38a6d7c1861f5038db a4e441ca7683ca SHA256: 555d497a60f22e3857 fdeb3dfc53aa86d059 26023c68c916d15d2d c3df6525bd
EFA 1.22.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.22.1.tar.gz	MD5: 600c0ad7cdbc06e8e8 46cb763f92901b SHA256: f90f3d5f59c031b9a9 64466b5401e86fd042 9272408f6c207c3f90 48254e9665
EFA 1.22.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.22.0.tar.gz	MD5: 8f100c93dc8ab519c2 aeb5dab89e98f8 SHA256: f329e7d54a86a03ea5 1da6ea9a5b68fb354f bae4a57a02f9592e21 fce431dc3a

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1.21.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.21.0.tar.gz	MD5: 959ccc3a4347461909 ec02ed3ba7c372 SHA256: c64e6ca34ccfc3ebe8 e82d08899ae8442b3e f552541cf5429c43d1 1a04333050
EFA 1.20.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.20.0.tar.gz	MD5: 7ebfbb8e85f1b94709 df4ab3db47913b SHA256: aeefd2681ffd5c4c63 1d1502867db5b83162 1d6eb85b61fe3ec80d f983d1dcf0
EFA 1.19.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.19.0.tar.gz	MD5: 2fd45324953347ec55 18da7e3fefa0ec SHA256: 99b77821b9e72c8dea 015cc92c96193e8db3 07deee05b91a58094c c331f16709
EFA 1.18.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.18.0.tar.gz	MD5: fc2571a72f5d3c7b7b 576ce2de38d91e SHA256: acb18a0808aedb9a5e 485f1469225b9ac97f 21db9af78e4cd69397 00debe1cb6

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1.17.3	https://efa-installer.amazonaws.com/ aws-efa-installer-1.17.3.tar.gz	MD5: 0517df4a190356ab55 9235147174cafd SHA256: 5130998b0d2883bbae 189b21ab215ecbc1b0 1ae0231659a9b4a17b 0a33ebc6ca
EFA 1.17.2	https://efa-installer.amazonaws.com/ aws-efa-installer-1.17.2.tar.gz	MD5: a329dedab53c4832df 218a24449f4c9a SHA256: bca1fdde8b32b00346 e175e597ffab32a09a 08ee9ab136875fb382 83cc4cd099
EFA 1.17.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.17.1.tar.gz	MD5: 733ae2cfc9d14b5201 7eaf0a2ab6b0ff SHA256: f29322640a88ae9279 805993cb836276ea24 0623820848463ca686 c8ce02136f
EFA 1.17.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.17.0.tar.gz	MD5: d430fc841563c11c38 05c5f82a4746b1 SHA256: 75ab0cee4fb6bd3888 9dce313183f5d3a83b d233e0a6ef6205d835 2821ea901d

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1.16.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.16.0.tar.gz	MD5: 399548d3b0d2e812d7 4dd67937b696b4 SHA256: cecec36495a1bc6fdc 82f97761a541e4fb6c 9a3cbf3cfcb145acf2 5ea5dbd45b
EFA 1.15.2	https://efa-installer.amazonaws.com/ aws-efa-installer-1.15.2.tar.gz	MD5: 955fea580d5170b058 23d51acde7ca21 SHA256: 84df4fbc1b3741b6c0 73176287789a601a58 9313accc8e6653434e 8d4c20bd49
EFA 1.15.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.15.1.tar.gz	MD5: c4610267039f72bbe4 e35d7bf53519bc SHA256: be871781a1b9a15fca 342a9d169219260069 942a8bda7a8ad06d4b aeb5e2efd7
EFA 1.15.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.15.0.tar.gz	MD5: 9861694e1cc00d884f adac07d22898be SHA256: b329862dd5729d2d09 8d0507fb486bf859d7 c70ce18b61c3029822 34a3a5c88f

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1.14.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.14.1.tar.gz	MD5: 50ba56397d359e5787 2fde1f74d4168a SHA256: c7b1b48e86fe4b3eaa 4299d3600930919c4f e6d88cc6e2c7e4a408 a3f16452c7
EFA 1.14.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.14.0.tar.gz	MD5: 40805e7fd842c36ece cb9fd7f921b1ae SHA256: 662d62c12de85116df 33780d40e0533ef7da d92709f4f613907475 a7a1b60a97
EFA 1.13.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.13.0.tar.gz	MD5: c91d16556f4fd53bec adbb345828221e SHA256: ad6705eb23a3fce44a f3afc0f76430915956 53a723ad0374084f4f 2b715192e1
EFA 1.12.3	https://efa-installer.amazonaws.com/ aws-efa-installer-1.12.3.tar.gz	MD5: 818aee81f097918cfa ebd724eddea678 SHA256: 2c225321824788b8ca 3fbc118207b944cdb0 96b847e1e0d1d853ef 2f0d727172

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1.12.2	https://efa-installer.amazonaws.com/ aws-efa-installer-1.12.2.tar.gz	MD5: 956bb1fc5ae0d6f0f8 7d2e481d49fccf SHA256: 083a868a2c212a5a4f cf3e4d732b685ce39c ceb3ca7e5d50d0b74e 7788d06259
EFA 1.12.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.12.1.tar.gz	MD5: f5bfe52779df435188 b0a2874d0633ea SHA256: 5665795c2b4f09d5f3 f767506d4d4c429695 b36d4a17e5758b27f0 33aee58900
EFA 1.12.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.12.0.tar.gz	MD5: d6c6b49fafb39b7702 97e1cc44fe68a6 SHA256: 28256c57e9ecc0b077 8b41c1f777a9982b4e 8eae782343dfe12460 79933dca59
EFA 1.11.2	https://efa-installer.amazonaws.com/ aws-efa-installer-1.11.2.tar.gz	MD5: 2376cf18d1353a4551 e35c33d269c404 SHA256: a25786f98a3628f7f5 4f7f74ee2b39bc6734 ea9374720507d37d3e 8bf8ee1371

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1.11.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.11.1.tar.gz	MD5: 026b0d9a0a48780cc7 406bd51997b1c0 SHA256: 6cb04baf5ffc58ddf3 19e956b5461289199c 8dd805fe216f8f9ab8 d102f6d02a
EFA 1.11.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.11.0.tar.gz	MD5: 7d9058e010ad65bf2e 14259214a36949 SHA256: 7891f6d45ae33e8221 89511c4ea1d14c9d54 d000f6696f97be54e9 15ce2c9dfa
EFA 1.10.1	https://efa-installer.amazonaws.com/ aws-efa-installer-1.10.1.tar.gz	MD5: 78521d3d668be22976 f46c6fecc7b730 SHA256: 61564582de7320b21d e319f532c3a677d26c c46785378eb3b95c63 6506b9bcb4
EFA 1.10.0	https://efa-installer.amazonaws.com/ aws-efa-installer-1.10.0.tar.gz	MD5: 46f73f5a7afe41b4bb 918c81888fef9a9 SHA256: 136612f96f2a085a7d 98296da0afb6fa807b 38142e2fc0c548fa98 6c41186282

Version	Télécharger le kit URL	Totaux de contrôle
EFA 1.9.5	https://efa-installer.amazonaws.com/ aws-efa-installer-1.9.5.tar.gz	MD5: 95edb8a209c18ba8d2 50409846eb6ef4 SHA256: a4343308d7ea4dc943 ccc21bcebed913e886 8e59bfb2ac93599c61 a7c87d7d25
EFA 1.9.4	https://efa-installer.amazonaws.com/ aws-efa-installer-1.9.4.tar.gz	MD5: f26dd5c350422c1a98 5e35947fa5aa28 SHA256: 1009b5182693490d90 8ef0ed2c1dd4f813cc 310a5d2062ce9619c4 c12b5a7f14
EFA 1.9.3	https://efa-installer.amazonaws.com/ aws-efa-installer-1.9.3.tar.gz	MD5: 95755765a097802d3e 6d5018d1a5d3d6 SHA256: 46ce732d6f3fcc9edf 6a6e9f9df0ad136054 328e24675567f7029e dab90c68f1
EFA 1.8.4	https://efa-installer.amazonaws.com/ aws-efa-installer-1.8.4.tar.gz	MD5: 85d594c41e831afc6c 9305263140457e SHA256: 0d974655a09b213d78 59e658965e56dc4f23 a0eee2dc44bb41b6d0 39cc5bab45

Topologie d'instance Amazon EC2

La description de la topologie de votre instance fournit une vue hiérarchique de la proximité relative entre les instances. Vous pouvez utiliser ces informations pour gérer l'infrastructure informatique de

calcul à haute performance (HPC) et d'apprentissage automatique (ML) à grande échelle, tout en optimisant le placement professionnel. Les tâches de HPC et de ML sont sensibles à la latence et au débit. Vous pouvez utiliser la topologie des instances pour détecter l'emplacement de vos instances, puis utiliser ces informations pour optimiser les tâches HPC et ML en les exécutant sur des instances physiquement plus proches les unes des autres.

Vous pouvez utiliser la topologie d'instance pour détecter l'emplacement de vos instances existantes, mais vous ne pouvez pas l'utiliser pour choisir de lancer une nouvelle instance physiquement proche d'une instance existante. Pour influencer le placement des instances, vous pouvez utiliser [Réserves de capacité dans des groupes de placement de cluster](#).

Tarifification

La description de la topologie de votre instance n'entraîne aucun coût supplémentaire.

Table des matières

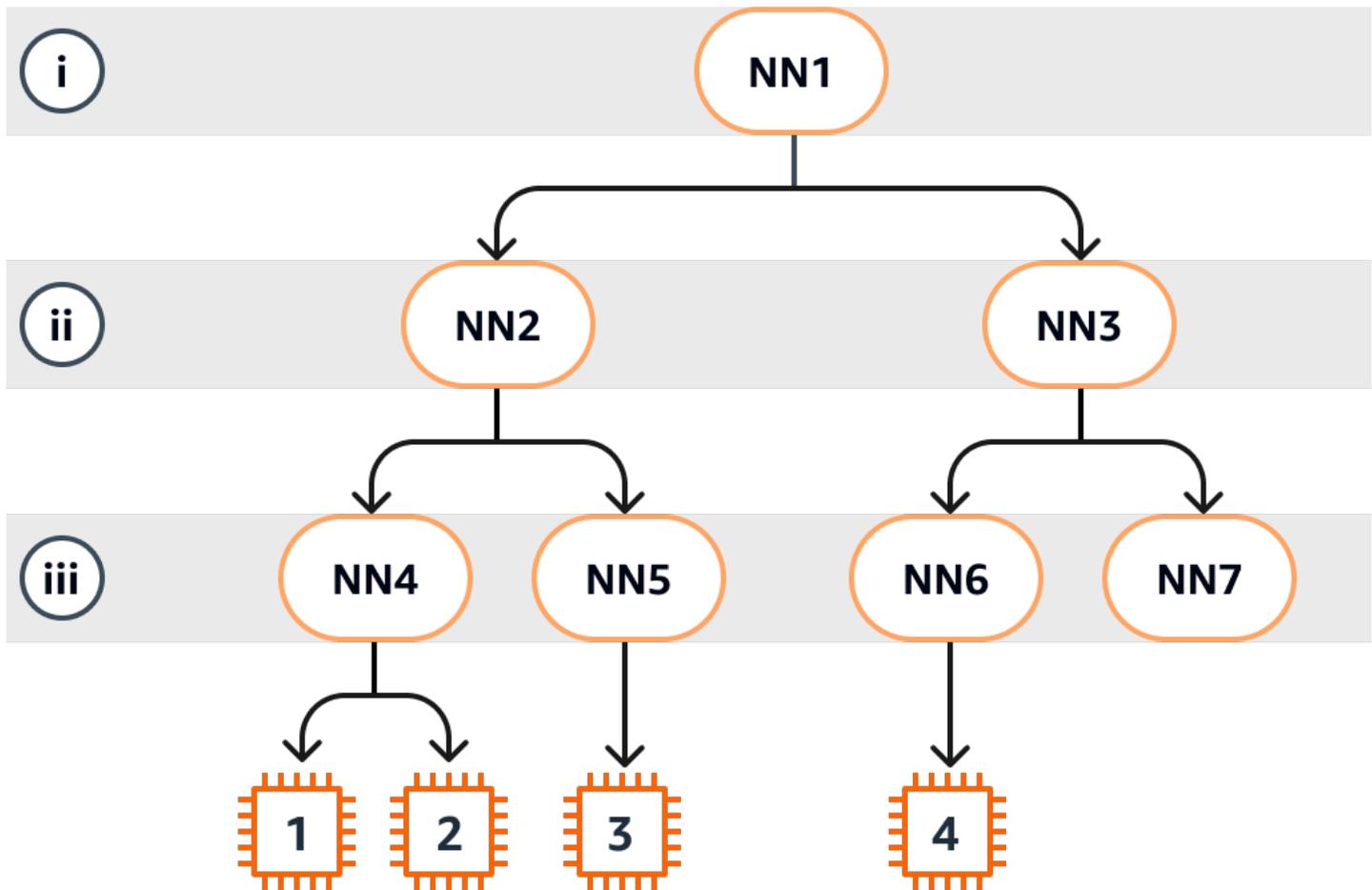
- [Fonctionnement de la topologie d'instance](#)
- [Conditions requises pour la topologie des instances](#)
- [Exemples de topologie d'instance Amazon EC2](#)

Fonctionnement de la topologie d'instance

Chaque instance EC2 se connecte à un ensemble de nœuds. Un ensemble de nœuds comprend trois nœuds de réseau, chaque nœud représentant une couche différente du AWS réseau. Les couches du réseau sont organisées selon une hiérarchie de 3 couches ou plus. L'ensemble de nœuds fournit une vue de haut en bas de cette hiérarchie, la couche inférieure étant connectée la plus proche d'une instance.

Les informations relatives à l'ensemble de nœuds sont appelées topologie d'instance.

Le schéma suivant fournit une représentation visuelle que vous pouvez utiliser pour comprendre la topologie de l'instance. Les nœuds du réseau sont identifiés comme NN1 — NN7. Les chiffres i, ii et iii identifient les couches du réseau. Les chiffres 1, 2, 3 et 4 identifient les instances EC2. Les instances se connectent à un nœud de la couche inférieure, identifié par iii. Plusieurs instances peuvent se connecter au même nœud.



Dans cet exemple :

- L'instance 1 se connecte au nœud de réseau 4 (NN4) de la couche iii. NN4 se connecte au nœud de réseau 2 (NN2) dans la couche ii, et NN2 se connecte au nœud de réseau 1 (NN1) dans la couche i, qui est le haut de la hiérarchie du réseau dans cet exemple. L'ensemble de nœuds de réseau comprend NN1, NN2 et NN4, exprimés hiérarchiquement des couches supérieures à la couche inférieure.
- L'instance 2 se connecte également au nœud de réseau 4 (NN4). L'instance 1 et l'instance 2 partagent le même ensemble de nœuds de réseau : NN1, NN2 et NN4.
- L'instance 3 se connecte au nœud de réseau 5 (NN5). NN5 se connecte à NN2, et NN2 se connecte à NN1. Le nœud de réseau défini pour l'instance 3 est NN1, NN2 et NN5.
- L'instance 4 se connecte au nœud de réseau 6 (NN6). Son ensemble de nœuds de réseau est NN1, NN3 et NN6.

Si l'on regarde la proximité des instances 1, 2 et 3, les instances 1 et 2 sont plus proches l'une de l'autre, car elles se connectent au même nœud de réseau (NN4), tandis que l'instance 3 est plus éloignée, car elle se connecte à un autre nœud de réseau (NN5).

Si l'on regarde la proximité de toutes les instances de ce schéma, les instances 1, 2 et 3 sont plus proches les unes des autres que de l'instance 4, car elles partagent le NN2 dans leur ensemble de nœuds de réseau.

En règle générale, si le nœud de réseau connecté à deux instances est le même, ces instances sont physiquement proches l'une de l'autre, comme c'est le cas pour les instances 1 et 2. En outre, moins il y a de sauts entre les nœuds de réseau, plus les instances sont proches les unes des autres. Par exemple, les instances 1 et 3 ont moins de sauts vers un nœud de réseau commun (NN2) que vers le nœud de réseau (NN1) qu'elles ont en commun avec l'instance 4, et sont donc plus proches l'une de l'autre qu'elles ne le sont de l'instance 4.

Aucune instance ne s'exécute sous le nœud de réseau 7 (NN7) dans cet exemple, et la sortie de l'API n'inclura donc pas NN7.

Comment interpréter le résultat

Vous obtenez les informations de topologie de l'instance à l'aide de l'API [DescribeInstanceTopology](#). La sortie fournit une vue hiérarchique de la topologie du réseau sous-jacent pour une instance.

L'exemple de sortie suivant correspond aux informations de topologie de réseau des quatre instances du schéma précédent. Les commentaires sont inclus dans l'exemple de sortie pour les besoins de cet exemple.

Il est important de noter les informations suivantes figurant dans la sortie :

- `NetworkNodes` décrit l'ensemble de nœuds de réseau d'une instance.
- Dans chaque ensemble de nœuds de réseau, les nœuds de réseau sont répertoriés par ordre hiérarchique de haut en bas.
- Le nœud de réseau connecté à l'instance est le dernier nœud de réseau de la liste (la couche inférieure).
- Pour déterminer quelles instances sont proches les unes des autres, recherchez d'abord les nœuds de réseau communs dans la couche inférieure. S'il n'existe aucun nœud de réseau commun dans la couche inférieure, recherchez des nœuds de réseau communs dans les couches supérieures.

Dans l'exemple de sortie suivant, `i-1111111111example` et `i-2222222222example` sont situées le plus près les uns des autres par rapport aux autres instances de cet exemple, car elles ont le nœud de réseau `nn-4444444444example` en commun dans la couche inférieure.

```
{
  "Instances": [
    {
      "InstanceId": "i-1111111111example", //Corresponds to instance 1
      "InstanceType": "p4d.24xlarge",
      "GroupName": "ML-group",
      "NetworkNodes": [
        "nn-1111111111example", //Corresponds to NN1 in layer i
        "nn-2222222222example", //Corresponds to NN2 in layer ii
        "nn-4444444444example" //Corresponds to NN4 in layer iii -
        bottom layer, connected to the instance
      ],
      "ZoneId": "usw2-az2",
      "AvailabilityZone": "us-west-2a"
    },
    {
      "InstanceId": "i-2222222222example", //Corresponds to instance 2
      "InstanceType": "p4d.24xlarge",
      "NetworkNodes": [
        "nn-1111111111example", //Corresponds to NN1 - layer i
        "nn-2222222222example", //Corresponds to NN2 - layer ii
        "nn-4444444444example" //Corresponds to NN4 - layer iii -
        connected to instance
      ],
      "ZoneId": "usw2-az2",
      "AvailabilityZone": "us-west-2a"
    },
    {
      "InstanceId": "i-3333333333example", //Corresponds to instance 3
      "InstanceType": "trn1.32xlarge",
      "NetworkNodes": [
        "nn-1111111111example", //Corresponds to NN1 - layer i
        "nn-2222222222example", //Corresponds to NN2 - layer ii
        "nn-5555555555example" //Corresponds to NN5 - layer iii -
        connected to instance
      ],
      "ZoneId": "usw2-az2",
      "AvailabilityZone": "us-west-2a"
    },
  ],
}
```

```
{
  "InstanceId": "i-444444444example", //Corresponds to instance 4
  "InstanceType": "trn1.2xlarge",
  "NetworkNodes": [
    "nn-111111111example", //Corresponds to NN1 - layer i
    "nn-333333333example", //Corresponds to NN3 - layer ii
    "nn-666666666example" //Corresponds to NN6 - layer iii -
connected to instance
  ],
  "ZoneId": "usw2-az2",
  "AvailabilityZone": "us-west-2a"
},
"NextToken": "SomeEncryptedToken"
}
```

Limites

Les limites suivantes s'appliquent :

- Les instances doivent être conformes à l'état `running`.
- Chaque vue de topologie d'instance est unique par compte.
- AWS Management Console ne prend pas en charge l'affichage de la topologie de l'instance.

Conditions requises pour la topologie des instances

Avant de décrire la topologie de vos instances, assurez-vous que celles-ci répondent aux exigences suivantes.

Exigences relatives à la description de la topologie de vos instances

- [Régions AWS](#)
- [Types d'instances](#)
- [État de l'instance](#)
- [Autorisation IAM](#)

Régions AWS

Soutenu Régions AWS :

- USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Californie du Nord), USA Ouest (Oregon)
- Asie-Pacifique (Séoul), Asie-Pacifique (Tokyo)
- Canada (Centre)
- Europe (Francfort), Europe (Irlande), Europe (Stockholm)

Types d'instances

Types d'instances pris en charge :

- hpc6a.48xlarge | hpc6id.32xlarge | hpc7a.12xlarge | hpc7a.24xlarge | hpc7a.48xlarge | hpc7a.96xlarge | hpc7g.4xlarge | hpc7g.8xlarge | hpc7g.16xlarge
- p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge | p5.48xlarge
- trn1.2xlarge | trn1.32xlarge | trn1n.32xlarge

Pour consulter les types d'instance disponibles dans une région spécifique

Les types d'instance disponibles varient selon la région. Pour voir si un type d'instance est disponible dans une région, utilisez la commande [describe-instance-types-offerings](#) avec le paramètre `--region`. Incluez le paramètre `--filters` pour étendre les résultats à la famille d'instances ou au type d'instance qui vous intéresse et le paramètre `--query` pour étendre la sortie à la valeur de `InstanceType`.

```
aws ec2 describe-instance-type-offerings \  
  --region us-east-2 \  
  --filters 'Name=instance-type, Values=trn1*' \  
  --query 'InstanceTypeOfferings[].InstanceType'
```

Sortie attendue

```
[  
  "trn1.2xlarge",  
  "trn1.32xlarge",  
  "trn1n.32xlarge"  
]
```

État de l'instance

Les instances doivent être dans l'état `running`. Vous ne pouvez pas obtenir d'informations sur la topologie des instances qui se trouvent dans un autre état.

Autorisation IAM

Votre identité IAM (utilisateur, groupe d'utilisateurs ou rôle) nécessite l'autorisation IAM suivante :

- `ec2:DescribeInstanceTopology`

Exemples de topologie d'instance Amazon EC2

Vous pouvez utiliser la commande [describe-instance-topology](#) CLI pour décrire la topologie d'instance de vos instances EC2.

Lorsque vous utilisez la commande `describe-instance-topology` sans paramètres ni filtres, la réponse inclut toutes vos instances qui correspondent aux types d'instances pris en charge pour cette commande dans la région spécifiée. Vous pouvez spécifier la région en incluant le paramètre `--region` ou en définissant une région par défaut. Pour plus d'informations sur la définition d'une région par défaut, consultez [Spécifier la région pour une ressource](#).

Vous pouvez inclure des paramètres pour renvoyer des instances qui correspondent aux ID d'instance ou aux noms de groupes de placement spécifiés. Vous pouvez également inclure des filtres pour renvoyer des instances correspondant à un type d'instance ou à une famille d'instances spécifiques, ou des instances situées dans une zone de disponibilité ou une zone locale spécifiée. Vous pouvez inclure un seul paramètre ou filtre, ou une combinaison de paramètres et de filtres.

La sortie est paginée, avec un maximum de 20 instances par page par défaut. Vous pouvez spécifier jusqu'à 100 instances par page à l'aide du paramètre `--max-results`.

Pour plus d'informations, consultez la section [describe-instance-topology](#) dans la référence des commandes AWS CLI .

Autorisations nécessaires

L'autorisation suivante est requise pour décrire la topologie de l'instance :

- `ec2:DescribeInstanceTopology`

Exemples

- [Exemple 1 : pas de paramètre ni de filtre](#)
- [Exemple 2 : filtre de type d'instance](#)
 - [Exemple 2a : filtre de correspondance exacte pour un type d'instance spécifié](#)
 - [Exemple 2b : filtre générique pour une famille d'instances](#)
 - [Exemple 2c : famille d'instances combinée et filtres de correspondance exacte](#)
- [Exemple 3 : filtre zone-id](#)
 - [Exemple 3a : filtre de zone de disponibilité](#)
 - [Exemple 3b : filtre de zone locale](#)
 - [Exemple 3c : combinaison des filtres de zone de disponibilité et de zone locale](#)
- [Exemple 4 : combinaison des filtres de type d'instance et zone-id](#)
- [Exemple 5 : paramètre de nom du groupe de placement](#)
- [Exemple 6 : ID d'instance](#)

Exemple 1 : pas de paramètre ni de filtre

Pour décrire la topologie de toutes vos instances

Utilisez la commande [describe-instance-topology](#) de la CLI sans spécifier de paramètres ni de filtres.

```
aws ec2 describe-instance-topology --region us-west-2
```

La réponse renvoie uniquement les instances qui correspondent aux types d'instances pris en charge pour cette API. Les instances peuvent se trouver dans différentes zones de disponibilité, zones locales (ZoneId) et groupes de placement (GroupName). Si une instance ne figure pas dans un groupe de placement, le champ GroupName n'apparaît pas dans la sortie. Dans l'exemple de sortie suivant, une seule instance se trouve dans un groupe de placement.

Exemple de sortie

```
{
  "Instances": [
    {
      "InstanceId": "i-1111111111example",
      "InstanceType": "p4d.24xlarge",
      "GroupName": "my-ml-cpg",
```

```
    "NetworkNodes": [
      "nn-1111111111example",
      "nn-2222222222example",
      "nn-3333333333example"
    ],
    "ZoneId": "usw2-az2",
    "AvailabilityZone": "us-west-2a"
  },
  {
    "InstanceId": "i-2222222222example",
    "InstanceType": "p4d.24xlarge",
    "NetworkNodes": [
      "nn-1111111111example",
      "nn-2222222222example",
      "nn-3333333333example"
    ],
    "ZoneId": "usw2-az2",
    "AvailabilityZone": "us-west-2a"
  },
  {
    "InstanceId": "i-3333333333example",
    "InstanceType": "trn1.32xlarge",
    "NetworkNodes": [
      "nn-1212121212example",
      "nn-1211122211example",
      "nn-1311133311example"
    ],
    "ZoneId": "usw2-az4",
    "AvailabilityZone": "us-west-2d"
  },
  {
    "InstanceId": "i-4444444444example",
    "InstanceType": "trn1.2xlarge",
    "NetworkNodes": [
      "nn-1111111111example",
      "nn-5434334334example",
      "nn-1235301234example"
    ],
    "ZoneId": "usw2-az2",
    "AvailabilityZone": "us-west-2a"
  }
],
"NextToken": "SomeEncryptedToken"
```

```
}
```

Exemple 2 : filtre de type d'instance

Vous pouvez filtrer en fonction d'un type d'instance spécifié (correspondance exacte) ou en fonction d'une famille d'instances (à l'aide d'un caractère générique). Vous pouvez également combiner un filtre de type d'instance et un filtre de famille d'instances spécifiés.

Exemple 2a : filtre de correspondance exacte pour un type d'instance spécifié

Pour décrire la topologie d'instance de toutes vos instances correspondant à un type d'instance spécifié

Utilisez la commande [describe-instance-topology](#) de la CLI avec le filtre `instance-type`. Dans cet exemple, la sortie est filtrée pour les instances `trn1n.32xlarge`. La réponse renverra uniquement les instances correspondant au type d'instance spécifié.

```
aws ec2 describe-instance-topology \  
  --region us-west-2 \  
  --filters Name=instance-type,Values=trn1n.32xlarge
```

Exemple de sortie

```
{  
  "Instances": [  
    {  
      "InstanceId": "i-2222222222example",  
      "InstanceType": "trn1n.32xlarge",  
      "NetworkNodes": [  
        "nn-1111111111example",  
        "nn-2222222222example",  
        "nn-3333333333example"  
      ],  
      "ZoneId": "usw2-az2",  
      "AvailabilityZone": "us-west-2a"  
    }  
  ],  
  "NextToken": "SomeEncryptedToken"  
}
```

Exemple 2b : filtre générique pour une famille d'instances

Pour décrire la topologie d'instance de toutes vos instances correspondant à une famille d'instances

Utilisez la commande [describe-instance-topology](#) de la CLI avec le filtre `instance-type`. Dans cet exemple, la sortie est filtrée pour les instances `trn1*`. La réponse renverra uniquement les instances correspondant à la famille d'instances spécifiée.

```
aws ec2 describe-instance-topology \  
  --region us-west-2 \  
  --filters Name=instance-type,Values=trn1*
```

Exemple de sortie

```
{  
  "Instances": [  
    {  
      "InstanceId": "i-222222222example",  
      "InstanceType": "trn1n.32xlarge",  
      "NetworkNodes": [  
        "nn-111111111example",  
        "nn-222222222example",  
        "nn-333333333example"  
      ],  
      "ZoneId": "usw2-az2",  
      "AvailabilityZone": "us-west-2a"  
    },  
    {  
      "InstanceId": "i-333333333example",  
      "InstanceType": "trn1.32xlarge",  
      "NetworkNodes": [  
        "nn-121212121example",  
        "nn-1211122211example",  
        "nn-1311133311example"  
      ],  
      "ZoneId": "usw2-az4",  
      "AvailabilityZone": "us-west-2d"  
    },  
    {  
      "InstanceId": "i-444444444example",  
      "InstanceType": "trn1.2xlarge",  
      "NetworkNodes": [  
        "nn-111111111example",
```

```

        "nn-5434334334example",
        "nn-1235301234example"
    ],
    "ZoneId": "usw2-az2",
    "AvailabilityZone": "us-west-2a"
}
],
"NextToken": "SomeEncryptedToken"
}

```

Exemple 2c : famille d'instances combinée et filtres de correspondance exacte

Pour décrire la topologie d'instance de toutes vos instances correspondant à une famille d'instances ou à un type d'instance spécifié

Utilisez la commande [describe-instance-topology](#) de la CLI avec le filtre `instance-type`. Dans cet exemple, la sortie est filtrée pour les instances `p4d*` ou `trn1n.32xlarge`. La réponse renverra les instances correspondant à n'importe lequel des filtres spécifiés.

```

aws ec2 describe-instance-topology \
  --region us-west-2 \
  --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"

```

Exemple de sortie

```

{
  "Instances": [
    {
      "InstanceId": "i-1111111111example",
      "InstanceType": "p4d.24xlarge",
      "GroupName": "ML-group",
      "NetworkNodes": [
        "nn-1111111111example",
        "nn-2222222222example",
        "nn-3333333333example"
      ],
      "ZoneId": "usw2-az2",
      "AvailabilityZone": "us-west-2a"
    },
    {
      "InstanceId": "i-2222222222example",
      "InstanceType": "trn1n.32xlarge",
      "NetworkNodes": [

```

```

        "nn-1111111111example",
        "nn-2222222222example",
        "nn-4343434343example"
    ],
    "ZoneId": "usw2-az2",
    "AvailabilityZone": "us-west-2a"
}
],
"NextToken": "SomeEncryptedToken"
}

```

Exemple 3 : filtre zone-id

Vous pouvez utiliser le filtre `zone-id` pour filtrer par zone de disponibilité ou zone locale. Vous pouvez également combiner le filtre de zone de disponibilité et le filtre de zone locale.

Exemple 3a : filtre de zone de disponibilité

Pour décrire la topologie d'instance de toutes vos instances correspondant à une zone de disponibilité spécifiée

Utilisez la commande [describe-instance-topology](#) de la CLI avec le filtre `zone-id`. Dans cet exemple, la sortie est filtrée à l'aide de l'ID de zone de disponibilité `use1-az1`. La réponse renverra uniquement les instances correspondant à la zone de disponibilité spécifiée.

```

aws ec2 describe-instance-topology \
  --region us-east-1 \
  --filters Name=zone-id,Values=use1-az1

```

Exemple de sortie

```

{
  "Instances": [
    {
      "InstanceId": "i-2222222222example",
      "InstanceType": "trn1n.32xlarge",
      "NetworkNodes": [
        "nn-1111111111example",
        "nn-2222222222example",
        "nn-3214313214example"
      ],
      "ZoneId": "use1-az1",
      "AvailabilityZone": "us-east-1a"
    }
  ]
}

```

```

    }
  ],
  "NextToken": "SomeEncryptedToken"
}

```

Exemple 3b : filtre de zone locale

Pour décrire la topologie d'instance de toutes vos instances correspondant à une zone locale spécifiée

Utilisez la commande [describe-instance-topology](#) de la CLI avec le filtre `zone-id`. Dans cet exemple, la sortie est filtrée à l'aide de l'ID de zone `use1-atl2-az1`. La réponse renverra uniquement les instances correspondant à la zone locale spécifiée.

```

aws ec2 describe-instance-topology \
  --region us-east-1 \
  --filters Name=zone-id,Values=use1-atl2-az1

```

Exemple de sortie

```

{
  "Instances": [
    {
      "InstanceId": "i-1111111111example",
      "InstanceType": "p4d.24xlarge",
      "GroupName": "ML-group",
      "NetworkNodes": [
        "nn-1111111111example",
        "nn-2222222222example",
        "nn-3333333333example"
      ],
      "ZoneId": "use1-atl2-az1",
      "AvailabilityZone": "us-east-1-atl-2a"
    }
  ],
  "NextToken": "SomeEncryptedToken"
}

```

Exemple 3c : combinaison des filtres de zone de disponibilité et de zone locale

Pour décrire la topologie d'instance de toutes vos instances correspondant à une zone de disponibilité ou une zone locale spécifiée

Utilisez la commande [describe-instance-topology](#) de la CLI avec le filtre `zone-id`. Dans cet exemple, la sortie est filtrée à l'aide de l'ID de zone de disponibilité `use1-az1` et de l'ID de zone locale `use1-atl2-az1`. La réponse renverra les instances correspondant à n'importe lequel des filtres spécifiés.

```
aws ec2 describe-instance-topology \  
  --region us-east-1 \  
  --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

Exemple de sortie

```
{  
  "Instances": [  
    {  
      "InstanceId": "i-1111111111example",  
      "InstanceType": "p4d.24xlarge",  
      "GroupName": "ML-group",  
      "NetworkNodes": [  
        "nn-1111111111example",  
        "nn-2222222222example",  
        "nn-3333333333example"  
      ],  
      "ZoneId": "use1-atl2-az1",  
      "AvailabilityZone": "us-east-1-atl-2a"  
    },  
    {  
      "InstanceId": "i-2222222222example",  
      "InstanceType": "trn1n.32xlarge",  
      "NetworkNodes": [  
        "nn-1111111111example",  
        "nn-2222222222example",  
        "nn-3214313214example"  
      ],  
      "ZoneId": "use1-az1",  
      "AvailabilityZone": "us-east-1a"  
    }  
  ],  
  "NextToken": "SomeEncryptedToken"  
}
```

Exemple 4 : combinaison des filtres de type d'instance et zone-id

Vous pouvez combiner tous les filtres au sein d'une même commande.

Pour décrire la topologie d'instance de toutes vos instances correspondant à un type d'instance, une famille d'instances, une zone de disponibilité ou une zone locale spécifiés

Utilisez la commande [describe-instance-topology](#) de la CLI avec les filtres `instance-type` et `zone-id`. Dans cet exemple, la sortie est filtrée en fonction de la famille d'`p4d*` instances, du type d'`trn1n.32xlarge` instance, de l'ID de zone de `use1-az1` disponibilité et de l'ID de zone `use1-atl2-az1` locale. La réponse renverra les instances qui correspondent aux instances `p4d*` ou `trn1n.32xlarge` situées dans les zones `us-east-1a` ou `us-east-1-atl-2a`.

```
aws ec2 describe-instance-topology \  
  --region us-east-1 \  
  --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" "Name=zone-  
id,Values=use1-az1,use1-atl2-az1"
```

Exemple de sortie

```
{  
  "Instances": [  
    {  
      "InstanceId": "i-1111111111example",  
      "InstanceType": "p4d.24xlarge",  
      "GroupName": "ML-group",  
      "NetworkNodes": [  
        "nn-1111111111example",  
        "nn-2222222222example",  
        "nn-3333333333example"  
      ],  
      "ZoneId": "use1-atl2-az1",  
      "AvailabilityZone": "us-east-1-atl-2a"  
    },  
    {  
      "InstanceId": "i-2222222222example",  
      "InstanceType": "trn1n.32xlarge",  
      "NetworkNodes": [  
        "nn-1111111111example",  
        "nn-2222222222example",  
        "nn-3214313214example"  
      ],  
      "ZoneId": "use1-az1",  
      "AvailabilityZone": "us-east-1a"  
    }  
  ],  
}
```

```
"NextToken": "SomeEncryptedToken"
}
```

Exemple 5 : paramètre de nom du groupe de placement

Pour décrire la topologie de toutes vos instances dans un groupe de placement spécifié

Utilisez la commande [describe-instance-topology](#) de la CLI avec le paramètre `group-names`. Dans l'exemple suivant, les instances peuvent se trouver dans le groupe de placement `ML-group` ou `HPC-group`. La réponse renverra les instances qui se trouvent dans l'un des groupes de placement.

```
aws ec2 describe-instance-topology \
  --region us-west-2 \
  --group-names ML-group HPC-group
```

Exemple de sortie

```
{
  "Instances": [
    {
      "InstanceId": "i-1111111111example",
      "InstanceType": "p4d.24xlarge",
      "GroupName": "ML-group",
      "NetworkNodes": [
        "nn-1111111111example",
        "nn-2222222222example",
        "nn-3333333333example"
      ],
      "ZoneId": "usw2-az2",
      "AvailabilityZone": "us-west-2a"
    },
    {
      "InstanceId": "i-2222222222example",
      "InstanceType": "trn1n.32xlarge",
      "GroupName": "HPC-group",
      "NetworkNodes": [
        "nn-1111111111example",
        "nn-2222222222example",
        "nn-3214313214example"
      ],
      "ZoneId": "usw2-az2",
      "AvailabilityZone": "us-west-2a"
    }
  ]
}
```

```
  ],  
  "NextToken": "SomeEncryptedToken"  
}
```

Exemple 6 : ID d'instance

Pour décrire la topologie d'instances spécifiées

Utilisez la commande [describe-instance-topology](#) de la CLI avec le paramètre `--instance-ids`. La réponse renverra les instances qui correspondent aux ID d'instance spécifiés.

```
aws ec2 describe-instance-topology \  
  --region us-west-2 \  
  --instance-ids i-1111111111example i-2222222222example
```

Exemple de sortie

```
{  
  "Instances": [  
    {  
      "InstanceId": "i-1111111111example",  
      "InstanceType": "p4d.24xlarge",  
      "GroupName": "ML-group",  
      "NetworkNodes": [  
        "nn-1111111111example",  
        "nn-2222222222example",  
        "nn-3333333333example"  
      ],  
      "ZoneId": "usw2-az2",  
      "AvailabilityZone": "us-west-2a"  
    },  
    {  
      "InstanceId": "i-2222222222example",  
      "InstanceType": "trn1n.32xlarge",  
      "GroupName": "HPC-group",  
      "NetworkNodes": [  
        "nn-1111111111example",  
        "nn-2222222222example",  
        "nn-3214313214example"  
      ],  
      "ZoneId": "usw2-az2",  
      "AvailabilityZone": "us-west-2a"  
    }  
  ]  
}
```

```
  ],  
  "NextToken": "SomeEncryptedToken"  
}
```

Groupes de placement

Pour répondre aux besoins de votre charge de travail, vous pouvez lancer un groupe d'instances EC2 interdépendantes dans un groupe de placement afin d'influencer leur placement.

Selon le type de charge de travail, vous pouvez créer un groupe de placement à l'aide de l'une des stratégies de placement suivantes :

- **Cluster** : regroupe des instances rapprochées à l'intérieur d'une Zone de disponibilité. Cette stratégie permet aux charges de travail d'atteindre les performances réseau à faible latence nécessaires aux node-to-node communications étroitement couplées, typiques des applications de calcul haute performance (HPC).
- **Partition** : répartit les instances entre les partitions logiques de façon à ce que des groupes d'instances d'une partition ne partagent pas le matériel sous-jacent avec des groupes d'instances d'autres partitions. Cette stratégie est généralement utilisée par les grandes charges de travail distribuées et répliquées telles que Hadoop, Cassandra, et Kafka.
- **Répartition** : place strictement un petit groupe d'instances sur un matériel sous-jacent distinct pour réduire les défaillances corrélées.

Les groupes de placement sont facultatifs. Si vous ne lancez pas vos instances dans un groupe de placement, EC2 tente de placer les instances de façon à ce que toutes vos instances soient réparties sur la matériel sous-jacent pour minimiser les échecs corrélés.

Il n'y a aucuns frais pour la création d'un groupe de placement.

Stratégies de placement

Vous pouvez créer un groupe de placement en employant l'une des stratégies de placement suivantes.

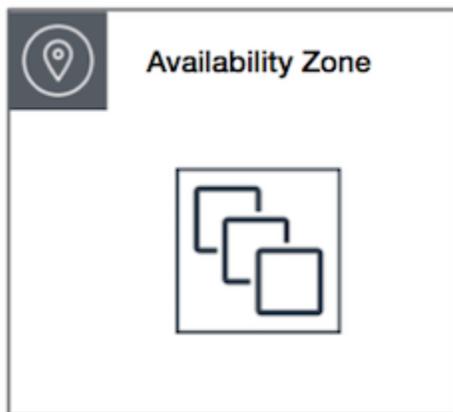
Stratégies de placement :

- [Groupes de placement du cluster](#)
- [Groupes de placement par partition](#)
- [Groupes de placement par répartition](#)

Groupes de placement du cluster

Un groupe de placement du cluster est un regroupement logique d'instances dans une même zone de disponibilité. Un groupe de placement du cluster peut s'étendre sur plusieurs réseaux privés virtuels (VPC) appairés dans la même région. Les instances du même groupe de placement de cluster bénéficient d'une limite de débit par flux supérieure pour le trafic TCP/IP et sont placées dans le même segment de bande passante haute bissection du réseau.

L'image ci-après illustre les instances placées dans un groupe de placement du cluster.



Les groupes de placement de cluster sont recommandés pour les applications qui bénéficient d'une latence réseau faible, d'un débit réseau élevé, ou des deux. Ils sont également recommandés lorsque la majorité du trafic réseau est échangé entre les instances du groupe. Pour fournir la latence la plus faible et les meilleures performances packet-per-second réseau à votre groupe de placement, choisissez un type d'instance qui prend en charge la mise en réseau améliorée. Pour plus d'informations, consultez [Gestion de réseau améliorée](#).

Nous vous recommandons de lancer vos instances de la façon suivante :

- Utilisez une seule demande de lancement pour lancer le nombre d'instances dont vous avez besoin dans le groupe de placement.
- Utilisez le même type d'instance pour toutes les instances du groupe de placement.

Si vous essayez d'ajouter ultérieurement des instances supplémentaires au groupe de placement, ou si vous essayez de lancer plusieurs types d'instance dans le groupe de placement, vous augmentez les risques d'obtenir une erreur de capacité insuffisante.

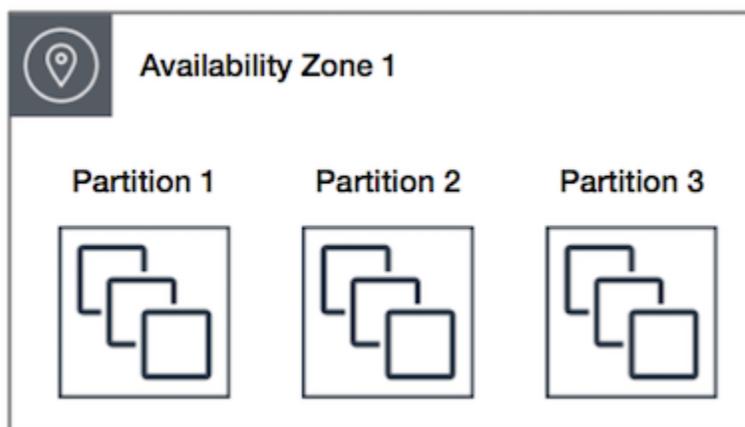
Si vous arrêtez une instance dans un groupe de placement, puis que vous la relancez, elle s'exécute encore au sein de celui-ci. Par contre, le démarrage échoue si la capacité est insuffisante pour l'instance.

Si vous recevez une erreur de capacité lorsque vous lancez une instance dans un groupe de placement dont des instances sont déjà en cours d'exécution, arrêtez et démarrez toutes les instances dans le groupe de placement, puis réessayez le lancement. Le redémarrage des instances peut entraîner leur migration vers un matériel qui dispose d'une capacité suffisante pour toutes les instances demandées.

Groupes de placement par partition

Les groupes de placement de partitions permettent de réduire la probabilité de défaillances de matériel corrélé pour votre application. Lorsque vous utilisez des groupes de placement de partitions, Amazon EC2 divise chaque groupe en segments logiques, appelés partitions. Amazon EC2 assure que chaque partition dans un groupe de placement dispose de son propre ensemble de racks. Chaque rack est doté de son propre réseau et de sa propre source d'alimentation. Aucune partition dans un même groupe de placement ne dispose du même portant, ce qui vous permet ainsi d'isoler l'impact d'échecs matériels dans votre application.

L'image suivante est une représentation visuelle simplifiée d'un groupe de placement de partitions dans une seule Zone de disponibilité. Elle représente des instances placées dans un groupe de placement par partition composé de trois partitions—Partition 1, Partition 2 et Partition 3. Chaque partition comprend plusieurs instances. Les instances d'une partition ne partagent pas de portants avec les instances des autres partitions, ce qui vous permet de limiter l'impact des pannes matérielles à une seule partition.



Il est possible d'utiliser les groupes de placement par partition afin de déployer des charges de travail distribuées et répliquées volumineuses (telles que HDFS, HBase et Cassandra) sur différents portants. Lorsque vous lancez des instances dans un groupe de placement par partition, Amazon EC2 tente de distribuer uniformément les instances sur toutes les partitions que vous spécifiez. Vous avez également la possibilité de lancer des instances d'une partition donnée afin de mieux contrôler l'emplacement des instances.

Un groupe de placement par partition peut disposer de partitions dans plusieurs Zones de disponibilité de la même région. Un groupe de placement par partition peut contenir jusqu'à sept partitions par zone de disponibilité. Seules les restrictions de votre compte limitent le nombre d'instances pouvant être lancées dans un groupe de placement par partition.

De plus, les groupes de placement par partition vous permettent de voir le détail des partitions — types d'instance présents dans telle ou telle partition. Vous pouvez partager ces informations avec des applications prenant en compte la topologie, telles que HDFS, HBase et Cassandra. Ces applications utilisent ces informations pour prendre des décisions informées sur la réplication des données dans le but d'accroître la disponibilité et la durabilité de ces dernières.

Si vous démarrez ou lancez une instance dans un groupe de placement par partition et que le matériel nécessaire au traitement de la demande est insuffisant, la demande échoue. Amazon EC2 met à disposition davantage de matériel distinct au fil du temps, vous pouvez donc renouveler votre demande plus tard.

Groupes de placement par répartition

Un groupe de placement par répartition est un groupe d'instances qui sont chacune placées sur du matériel distinct.

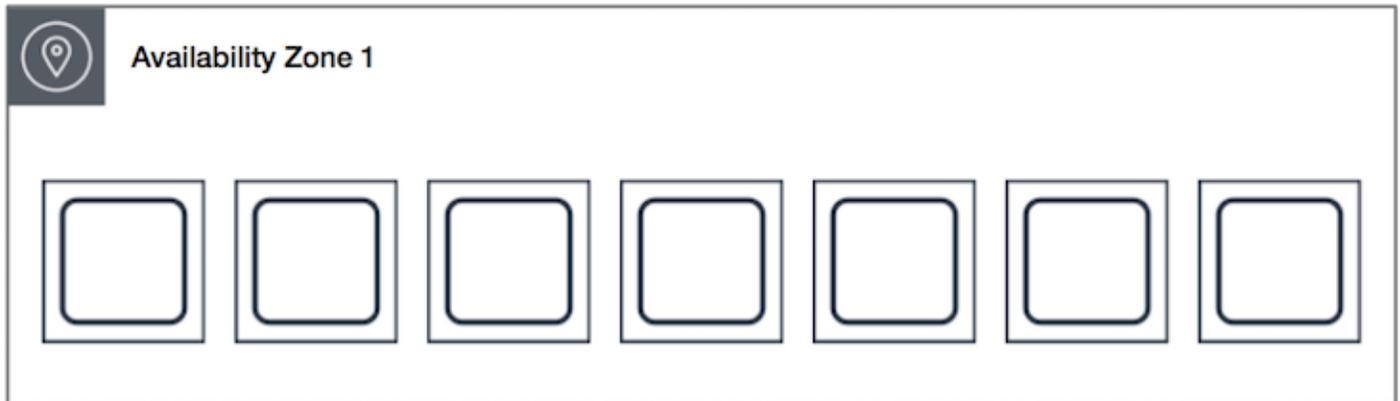
Les groupes de placement par répartition sont recommandés pour les applications ayant un petit nombre d'instances critiques, qui doivent être séparées les unes des autres. Le lancement d'instances dans un groupe de placement par répartition réduit le risque de défaillances simultanées, qui peuvent se produire lorsque les instances partagent le même matériel. Les groupes de placement par répartition fournissent un accès à du matériel distinct et sont par conséquent adaptés à l'association de différents types d'instance et au lancement d'instances au fil du temps.

Si vous démarrez ou lancez une instance dans un groupe de placement par répartition et que le matériel nécessaire au traitement de la demande est insuffisant, la demande échoue. Amazon EC2 met à disposition davantage de matériel distinct au fil du temps, vous pouvez donc renouveler votre demande plus tard. Les groupes de placement peuvent répartir des instances sur des racks ou

des hôtes. Les groupes de placement répartis au niveau du rack peuvent être utilisés dans AWS les régions et au-delà AWS Outposts. Les groupes de placement de spread au niveau de l'hôte ne peuvent être utilisés AWS Outposts qu'avec.

Groupes de placement répartis au niveau du rack

L'image ci-après représente sept instances au sein d'une seule zone de disponibilité qui sont placées dans un groupe de placement par répartition. Les sept instances sont placées sur sept racks différents, chaque rack ayant son propre réseau et sa propre source d'alimentation.



Un groupe de placement de spread au niveau du rack peut couvrir plusieurs zones de disponibilité dans la même région. Dans une région, un groupe de placement de spread au niveau du rack peut avoir un maximum de sept instances actives par zone de disponibilité et par groupe. Avec Outposts, un groupe de placement de spread au niveau du rack peut contenir autant d'instances que vous avez de racks dans votre déploiement d'Outposts.

Groupes de placement par répartition au niveau des hôtes

Les groupes de placement de spread au niveau de l'hôte ne sont disponibles qu'avec AWS Outposts. Un groupe de placement au niveau du spread d'hôtes peut contenir autant d'instances que vous avez d'hôtes dans votre déploiement Outpost. Pour plus d'informations, consultez [the section called "Groupes de placement sur AWS Outposts"](#).

Règles et restrictions des groupes de placement

Rubriques

- [Règles et restrictions générales](#)
- [Règles et restrictions des groupes de placement du cluster](#)

- [Règles et restrictions des groupes de placement par partition](#)
- [Règles et restrictions des groupes de placement par répartition](#)

Règles et restrictions générales

Avant d'utiliser des groupes de placement, vous devez être conscient des règles suivantes :

- Vous pouvez créer un maximum de 500 groupes de placement par compte dans chaque région.
- Le nom que vous spécifiez pour un groupe de placement doit être unique au sein de votre compte AWS pour la région.
- Vous ne pouvez pas fusionner des groupes de placement.
- Une instance peut être lancée dans un seul groupe de placement à la fois ; elle ne peut pas s'étendre sur plusieurs groupes de placement.
- [Les réservations de capacité à la demande](#) et les [instances réservées zonales](#) vous permettent de réserver de la capacité pour les instances EC2 dans les zones de disponibilité. Lorsque vous lancez une instance, si les attributs de l'instance correspondent à ceux spécifiés par une réservation de capacité à la demande ou une instance réservée zonale, la capacité réservée est automatiquement utilisée par l'instance. Cela est également vrai si vous lancez l'instance dans un groupe de placement.

Si vous envisagez de lancer des instances dans un groupe de placement de clusters, nous vous recommandons de réserver de la capacité de manière explicite dans le groupe de placement de clusters. Vous pouvez le faire en créant une [réservation de capacité à la demande dans un groupe de placement de clusters spécifié](#). Notez que même si vous pouvez réserver de la capacité de cette manière à l'aide des réservations de capacité à la demande, il n'en va pas de même pour les instances réservées zonales, car elles ne peuvent pas réserver de capacité de manière explicite dans un groupe de placement.

- Vous ne pouvez pas lancer d'hôtes dédiés dans des groupes de placement.
- Vous ne pouvez pas lancer une instance Spot configurée pour s'arrêter ou se mettre en veille prolongée en cas d'interruption dans un groupe de placement.

Règles et restrictions des groupes de placement du cluster

Les règles suivantes s'appliquent aux groupes de placement du cluster :

- Seuls les types d'instances suivants sont pris en charge :

- Instances de la génération actuelle, à l'exception des instances de [performance burstable](#) (par exemple, T2), des instances [Mac1 et des instances M7i-Flex](#).
- Les instances de génération précédente suivantes : A1, C3, C4, I2, M4, R3 et R4.
- Un groupe de placement du cluster ne peut pas s'étendre sur plusieurs zones de disponibilité.
- La vitesse de débit réseau maximale du trafic entre deux instances au sein d'un groupe de placement du cluster est limitée par la plus lente des deux instances. Pour les applications très exigeantes en débit, choisissez un type d'instance avec une connectivité réseau qui correspond à vos besoins.
- Pour les instances pour lesquelles la mise en réseau améliorée est active, les règles suivantes s'appliquent :
 - Les instances se trouvant dans un groupe de placement du cluster peuvent utiliser jusqu'à 10 Gbit/s pour le trafic à flux unique. Les instances qui ne se trouvent pas dans un groupe de placement du cluster peuvent utiliser jusqu'à 5 Gbit/s pour le trafic à flux unique.
 - Le trafic vers et depuis des compartiments Amazon S3 de la même région via l'espace d'adressage IP public ou un point de terminaison d'un VPC peut utiliser la totalité de la bande passante cumulée disponible pour l'instance.
- Vous pouvez lancer plusieurs types d'instance dans un groupe de placement du cluster. Toutefois, cela réduit la probabilité de disponibilité de la capacité requise pour que votre lancement réussisse. Nous vous recommandons d'utiliser le même type d'instance pour toutes les instances d'un groupe de placement du cluster.
- Le trafic réseau vers Internet et via une AWS Direct Connect connexion aux ressources locales est limité à 5 Gbit/s pour les groupes de placement de clusters.

Règles et restrictions des groupes de placement par partition

Les règles suivantes s'appliquent aux groupes de placement par partition :

- Un groupe de placement par partition prend en charge jusqu'à sept partitions par zone de disponibilité. Seules les restrictions de votre compte limitent le nombre d'instances pouvant être lancées dans un groupe de placement par partition.
- Lorsque vous lancez des instances dans un groupe de placement par partition, Amazon EC2 tente de distribuer uniformément les instances sur toutes les partitions. Amazon EC2 ne garantit pas une distribution uniforme des instances sur toutes les partitions.
- Un groupe de placement par partition avec des instances dédiées peut comprendre deux partitions au maximum.

- Les réservations de capacité ne réservent pas de capacité dans un groupe de placement par partition.

Règles et restrictions des groupes de placement par répartition

Les règles suivantes s'appliquent aux groupes de placement par répartition :

- Un groupe de placement par répartition sur de racks prend en charge un maximum de sept instances en cours d'exécution par zone de disponibilité. Par exemple, dans une région comportant trois zones de disponibilité, vous pouvez exécuter un total de 21 instances dans le groupe, avec sept instances dans chaque zone de disponibilité. Si vous essayez de lancer une huitième instance dans la même zone de disponibilité et dans le même groupe de placement par répartition, le lancement échoue. Si vous avez besoin de plus de sept instances dans une zone de disponibilité, nous vous recommandons d'utiliser plusieurs groupes de placement par répartition. L'utilisation de plusieurs groupes de placement par répartition ne garantit pas la répartition des instances entre les groupes, mais cela permet de garantir la répartition pour chaque groupe, limitant ainsi l'impact de certains types d'incidents.
- Les groupes de placement par répartition ne sont pas pris en charge pour les instances dédiées.
- Les groupes de placement de spread au niveau de l'hôte ne sont pris en charge que pour les groupes de placement activés AWS Outposts. Un groupe de placement de spread au niveau de l'hôte peut contenir autant d'instances que d'hôtes dans votre déploiement Outpost.
- Dans une région, un groupe de placement de spread au niveau du rack peut avoir un maximum de sept instances actives par zone de disponibilité et par groupe. Ainsi AWS Outposts, un groupe de placement de spread au niveau du rack peut contenir autant d'instances que vous avez de racks dans votre déploiement Outpost.
- Les réservations de capacité ne réservent pas de capacité dans un groupe de placement par répartition.

Utilisation des groupes de placement

Table des matières

- [Créer un groupe de placement.](#)
- [Afficher les informations sur le groupe de placement](#)
- [Baliser un groupe de placement](#)
- [Lancer des instances dans un groupe de placement](#)

- [Décrire des instances dans un groupe de placement](#)
- [Modifier le groupe de placement d'une instance](#)
- [Suppression d'une instance d'un groupe de placement](#)
- [Supprimer un groupe de placement](#)

Créer un groupe de placement.

Vous pouvez créer un groupe de placement en employant l'une des méthodes suivantes.

Console

Pour créer un groupe de placement à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de placement.
3. Choisissez Créer un groupe de placement.
4. Spécifiez le nom du groupe.
5. Choisissez la stratégie de placement du groupe.
 - Si vous choisissez Spread (Répartition), choisissez le niveau de répartition.
 - Rack : aucune restriction
 - Hôte : uniquement pour les Outposts
 - Si vous choisissez Partition, choisissez le nombre de partitions au sein du groupe.
6. Pour baliser le groupe de placement, choisissez Add tag (Ajouter une identification), puis saisissez une clé et une valeur. Choisissez Add tag (Ajouter une identification) pour chaque identification que vous voulez ajouter.
7. Choisissez Créer un groupe.

AWS CLI

Pour créer un groupe de placement à l'aide du AWS CLI

Utilisez la commande [create-placement-group](#). L'exemple suivant crée un groupe de placement nommé `my-cluster` qui utilise la stratégie de placement `cluster` et applique une balise avec une clé `purpose` et une valeur `production`.

```
aws ec2 create-placement-group \  
  --group-name my-cluster \  
  --strategy cluster \  
  --tag-specifications 'ResourceType=placement-  
group,Tags={Key=purpose,Value=production}'
```

Pour créer un groupe de placement de partitions à l'aide du AWS CLI

Utilisez la commande [create-placement-group](#). Spécifiez le paramètre `--strategy` avec la valeur `partition` et le paramètre `--partition-count` avec le nombre de partitions souhaité. Dans cet exemple, le groupe de placement par partition est nommé `HDFS-Group-A` et créé avec cinq partitions.

```
aws ec2 create-placement-group \  
  --group-name HDFS-Group-A \  
  --strategy partition \  
  --partition-count 5
```

PowerShell

Pour créer un groupe de placement à l'aide du AWS Tools for Windows PowerShell

Utilisez la commande [New-EC2PlacementGroup](#).

Afficher les informations sur le groupe de placement

Vous pouvez consulter tous vos groupes de placement et les informations les concernant à l'aide de l'une des méthodes suivantes.

Console

Pour afficher les informations relatives à un ou plusieurs groupes de placement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Réseau et sécurité, choisissez Placement Groups.
3. Dans le tableau Groupes de placement, pour chaque groupe de placement, vous pouvez consulter les informations suivantes :
 - Nom du groupe : nom que vous avez donné au groupe de placement.

- ID du groupe : ID du groupe de placement.
- Stratégie — Stratégie de placement pour le groupe de placement.
- État : état du groupe de placement.
- Partition : nombre de partitions. Valable uniquement si la stratégie est une partition.
- ARN du groupe : nom de ressource Amazon (ARN) du groupe de placement.

AWS CLI

Pour décrire tous vos groupes de placement

Utilisez la commande [AWS CLI describe-placement-groups](#).

```
aws ec2 describe-placement-groups
```

Exemple de réponse

```
{
  "PlacementGroups": [
    {
      "GroupName": "my-cluster-pg",
      "State": "available",
      "Strategy": "cluster",
      "GroupId": "pg-0123456789example",
      "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
    },
    ...
  ]
}
```

Pour décrire un groupe de placement spécifié

Utilisez la commande [AWS CLI describe-placement-groups](#). Vous pouvez spécifier le `--group-id` ou le `--group-name` paramètre.

Spécifiez l'ID du groupe de placement :

```
aws ec2 describe-placement-groups --group-id pg-0123456789example
```

Spécifiez le nom du groupe de placement :

```
aws ec2 describe-placement-groups --group-name my-cluster-pg
```

Exemple de réponse

```
{
  "PlacementGroups": [
    {
      "GroupName": "my-cluster-pg",
      "State": "available",
      "Strategy": "cluster",
      "GroupId": "pg-0123456789example",
      "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
    }
  ]
}
```

Baliser un groupe de placement

Pour vous aider à classer et à gérer vos groupes de placement existants, vous pouvez les baliser avec des métadonnées personnalisées. Pour plus d'informations sur le fonctionnement des balises, consultez [Baliser vos ressources Amazon EC2](#).

Lorsque vous balisez un groupe de placement, les instances lancées dans le groupe de placement ne sont pas automatiquement balisées. Vous devez baliser explicitement les instances lancées dans le groupe de placement. Pour plus d'informations, consultez [Ajouter une balise lorsque vous lancez une instance](#).

Vous pouvez afficher, ajouter et supprimer des étiquettes à l'aide de l'une des méthodes suivantes.

Console

Pour afficher, ajouter ou supprimer une balise pour un groupe de placement existant

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de placement.
3. Sélectionnez un groupe de placement, puis choisissez Actions, Gérer les balises.

4. L'écran Gérer les balises affiche toutes les balises affectées au groupe de placement.
 - Pour ajouter une balise, choisissez Ajouter la balise, puis entrez la clé et la valeur de la balise. Vous pouvez ajouter jusqu'à 50 balises par groupe de placement. Pour plus d'informations, consultez [Restrictions liées aux balises](#).
 - Pour supprimer une balise, choisissez Supprimer en regard de la balise à supprimer.
5. Choisissez Enregistrer.

AWS CLI

Pour afficher les balises des groupe de placement

Utilisez la commande [describe-tags](#) pour afficher les balises de la ressource spécifiée. Dans l'exemple suivant, vous décrivez les balises de tous vos groupes de placement.

```
aws ec2 describe-tags \  
  --filters Name=resource-type,Values=placement-group
```

```
{  
  "Tags": [  
    {  
      "Key": "Environment",  
      "ResourceId": "pg-0123456789EXAMPLE",  
      "ResourceType": "placement-group",  
      "Value": "Production"  
    },  
    {  
      "Key": "Environment",  
      "ResourceId": "pg-9876543210EXAMPLE",  
      "ResourceType": "placement-group",  
      "Value": "Production"  
    }  
  ]  
}
```

Vous pouvez également utiliser la commande [describe-tags](#) pour afficher les balises d'un groupe de placement en spécifiant son ID. Dans l'exemple suivant, vous décrivez les balises pour pg-0123456789EXAMPLE.

```
aws ec2 describe-tags \  
  --filters Name=resource-id,Values=pg-0123456789EXAMPLE
```

```
--filters Name=resource-id,Values=pg-0123456789EXAMPLE
```

```
{
  "Tags": [
    {
      "Key": "Environment",
      "ResourceId": "pg-0123456789EXAMPLE",
      "ResourceType": "placement-group",
      "Value": "Production"
    }
  ]
}
```

Vous pouvez également afficher les balises d'un groupe de placement en décrivant le groupe de placement.

Utilisez la commande [describe-placement-groups](#) pour afficher la configuration du groupe de placement spécifié, qui inclut toutes les balises définies pour le groupe de placement.

```
aws ec2 describe-placement-groups \
  --group-name my-cluster
```

```
{
  "PlacementGroups": [
    {
      "GroupName": "my-cluster",
      "State": "available",
      "Strategy": "cluster",
      "GroupId": "pg-0123456789EXAMPLE",
      "Tags": [
        {
          "Key": "Environment",
          "Value": "Production"
        }
      ]
    }
  ]
}
```

Pour étiqueter un groupe de placement existant à l'aide du AWS CLI

Utilisez la commande [create-tags](#) pour baliser les ressources existantes. Dans l'exemple suivant, le groupe de placement existant est étiqueté avec `Key=Cost-Center` et `Value=CC-123`.

```
aws ec2 create-tags \  
  --resources pg-0123456789EXAMPLE \  
  --tags Key=Cost-Center,Value=CC-123
```

Pour supprimer une étiquette d'un groupe de placement à l'aide du AWS CLI

Vous pouvez utiliser la commande [delete-tags](#) pour supprimer des balises de ressources existantes. Pour obtenir des exemples, reportez-vous à la section [Exemples](#) dans le document [AWS CLI Références des commandes](#).

PowerShell

Pour afficher les balises des groupe de placement

Utilisez la commande [Get-EC2Tag](#).

Pour décrire les balises d'un groupe de placement spécifique

Utilisez la commande [Get-EC2PlacementGroup](#).

Pour baliser un groupe de placement existant

Utilisez la commande [New-EC2Tag](#).

Pour supprimer une balise d'un groupe de placement

Utilisez la commande [Remove-EC2Tag](#).

Lancer des instances dans un groupe de placement

Vous pouvez lancer une instance dans un groupe de placement si les [règles et les limitations de groupe de placement sont respectées](#) en employant l'une des méthodes suivantes.

Console

Lancement d'instances dans un groupe de placement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Sur le tableau de bord de la console EC2, dans la case Lancer une instance, choisissez Lancer une instance. Remplissez le formulaire comme indiqué, en prenant soin de faire ce qui suit :
 - Sous Instance type (Type d'instance), sélectionnez un type d'instance qui peut être lancé dans un groupe de placement.
 - Dans la zone Summary (Résumé), sous Number of instances (Nombre d'instances), saisissez le nombre total d'instances dont vous avez besoin dans ce groupe de placement, car il se peut que vous ne puissiez pas ajouter d'instances au groupe de placement ultérieurement.
 - Sous Advanced details (Détails avancés), pour Placement group name (Nom du groupe de placement), vous pouvez choisir d'ajouter les instances à un groupe de placement nouveau ou existant. Si vous choisissez un groupe de placement avec une stratégie de partition, pour Target partition (Partition cible), choisissez la partition dans laquelle lancer les instances.

AWS CLI

Lancement d'instances dans un groupe de placement

Utilisez la commande [run-instances](#) et spécifiez le nom du groupe de placement à l'aide du paramètre `--placement` "GroupName = *my-cluster*". Dans cet exemple, le groupe de placement est nommé `my-cluster`.

```
aws ec2 run-instances --placement "GroupName = my-cluster"
```

Pour lancer des instances dans une partition spécifique d'un groupe de placement de partitions à l'aide du AWS CLI

Utilisez la commande [run-instances](#) et spécifiez le nom du groupe de placement et la partition à l'aide du paramètre `--placement` "GroupName = *HDFS-Group-A*, PartitionNumber = *3*". Dans cet exemple, le groupe de placement est nommé `HDFS-Group-A` et il contient 3 partitions.

```
aws ec2 run-instances --placement "GroupName = HDFS-Group-A, PartitionNumber = 3"
```

PowerShell

Pour lancer les instances dans un groupe de placement à l'aide d' AWS Tools for Windows PowerShell

Utilisez la [New-EC2Instance](#) commande et spécifiez le nom du groupe de placement à l'aide du `-Placement_GroupName` paramètre.

Décrire des instances dans un groupe de placement

Vous pouvez afficher les informations de placement de vos instances en employant l'une des méthodes suivantes. Vous pouvez également filtrer les groupes de placement par partition par nombre de partitions à l'aide de l' AWS CLI.

Console

Affichage du groupe de placement et du nombre de partitions d'une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Dans l'onglet Details (Détails) sous Host and placement group (Hôte et groupe de placement), recherchez Placement group (Groupe de placement). Le champ est vide si l'instance ne figure pas dans un groupe de placement. Sinon, il contient le nom du groupe de placement. Si le groupe de placement est un groupe de placement, Numéro de partition contient le numéro de partition de l'instance.

AWS CLI

Affichage du nombre de partitions d'une instance dans un groupe de placement de partitions

Utilisez la commande [describe-instances](#) et spécifiez le paramètre `--instance-id`.

```
aws ec2 describe-instances --instance-id i-0123a456700123456
```

La réponse inclut les informations sur le placement, notamment le nom du groupe de placement et le nombre de partitions correspondant à l'instance.

```
"Placement": {
```

```
"AvailabilityZone": "us-east-1c",
"GroupName": "HDFS-Group-A",
"PartitionNumber": 3,
"Tenancy": "default"
}
```

Filtrage des instances pour un groupe de placement de partitions et un nombre de partitions

Utilisez la commande [describe-instances](#) et spécifiez le paramètre `--filters` avec les filtres `placement-group-name` et `placement-partition-number`. Dans cet exemple, le groupe de placement est nommé `HDFS-Group-A` et il contient 7 partitions.

```
aws ec2 describe-instances --filters "Name = placement-group-name, Values = HDFS-Group-A" "Name = placement-partition-number, Values = 7"
```

La réponse répertorie toutes les instances qui figurent dans la partition désignée au sein du groupe de placement spécifié. Voici un exemple de sortie présentant uniquement l'ID et le type d'instance ainsi que les informations sur le placement pour les instances retournées.

```
"Instances": [
  {
    "InstanceId": "i-0a1bc23d4567e8f90",
    "InstanceType": "r4.large",
  },
  "Placement": {
    "AvailabilityZone": "us-east-1c",
    "GroupName": "HDFS-Group-A",
    "PartitionNumber": 7,
    "Tenancy": "default"
  }
  {
    "InstanceId": "i-0a9b876cd5d4ef321",
    "InstanceType": "r4.large",
  },
  "Placement": {
    "AvailabilityZone": "us-east-1c",
    "GroupName": "HDFS-Group-A",
    "PartitionNumber": 7,
    "Tenancy": "default"
  }
}
```

```
    ],  
  }  
}
```

Modifier le groupe de placement d'une instance

Vous pouvez modifier le groupe de placement d'une instance comme suit :

- Déplacement d'une instance existante vers un groupe de placement
- Déplacement d'une instance d'un groupe de placement vers un autre

Avant de pouvoir déplacer l'instance, celle-ci doit être dans l'état `stopped`.

Console

Déplacement d'une instance vers un groupe de placement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez État de l'instance, Arrêter l'instance.
4. Tandis que l'instance est toujours sélectionnée, choisissez Actions, Paramètres de l'instance, puis Changer le placement d'instance.
5. Pour Groupe de placement, choisissez le groupe de placement vers lequel déplacer l'instance.
6. Choisissez Enregistrer.

AWS CLI

Déplacement d'une instance vers un groupe de placement

1. Arrêtez l'instance à l'aide de la commande [stop-instances](#).
2. Utilisez la commande [modify-instance-placement](#) et spécifiez le nom du groupe de placement vers lequel déplacer l'instance.

```
aws ec2 modify-instance-placement \  
  --instance-id i-0123a456700123456 \  
  --group-name MySpreadGroup
```

3. Démarrez l'instance à l'aide de la commande [start-instances](#).

PowerShell

Pour déplacer une instance vers un groupe de placement à l'aide de l' AWS Tools for Windows PowerShell

1. Arrêtez l'instance à l'aide de la [Stop-EC2Instance](#) commande.
2. Utilisez la [Edit-EC2InstancePlacement](#) commande et spécifiez le nom du groupe de placement vers lequel vous souhaitez déplacer l'instance.
3. Démarrez l'instance à l'aide de la [Start-EC2Instance](#) commande.

Suppression d'une instance d'un groupe de placement

Vous pouvez supprimer une instance d'un groupe de placement en utilisant l'une des méthodes suivantes.

Avant de pouvoir supprimer une instance d'un groupe de placement, l'instance doit être dans l'état stopped.

Console

Suppression d'une instance d'un groupe de placement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez État de l'instance, Arrêter l'instance.
4. Tandis que l'instance est toujours sélectionnée, choisissez Actions, Paramètres de l'instance, puis Changer le placement d'instance.
5. Pour Groupe de placement, choisissez Aucun.
6. Choisissez Enregistrer.

AWS CLI

Suppression d'une instance d'un groupe de placement

1. Arrêtez l'instance à l'aide de la commande [stop-instances](#).

2. Utilisez la commande [modify-instance-placement](#) et spécifiez une chaîne vide pour le nom du groupe.

```
aws ec2 modify-instance-placement \  
  --instance-id i-0123a456700123456 \  
  --group-name ""
```

3. Démarrez l'instance à l'aide de la commande [start-instances](#).

PowerShell

Pour supprimer une instance d'un groupe de placement à l'aide de l' AWS Tools for Windows PowerShell

1. Arrêtez l'instance à l'aide de la [Stop-EC2Instance](#) commande.
2. Utilisez la [Edit-EC2InstancePlacement](#) commande et spécifiez une chaîne vide pour le nom du groupe de placement.
3. Démarrez l'instance à l'aide de la [Start-EC2Instance](#) commande.

Supprimer un groupe de placement

Si vous avez besoin de supprimer un groupe de placement ou si vous n'en avez plus besoin, vous pouvez le supprimer. Vous pouvez supprimer un groupe de placement en employant l'une des méthodes suivantes.

Prérequis

Pour pouvoir être supprimé, un groupe de placement ne doit pas contenir d'instances. Vous pouvez [résilier](#) toutes les instances que vous avez lancées dans le groupe de placement, [déplacer](#) les instances dans un autre groupe de placement ou [supprimer](#) les instances du groupe de placement.

Console

Suppression d'un groupe de placement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de placement.
3. Sélectionnez le groupe de placement et choisissez Actions, Supprimer.

4. Lorsque vous êtes invité à confirmer, entrez **Delete**, puis choisissez Delete (Supprimer).

AWS CLI

Suppression d'un groupe de placement

Utilisez la commande [delete-placement-group](#) et indiquez le nom du groupe de placement à supprimer. Dans cet exemple, le nom du groupe de placement est `my-cluster`.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Pour supprimer un groupe de placement à l'aide du AWS Tools for Windows PowerShell

Utilisez la [Remove-EC2PlacementGroup](#) commande pour supprimer le groupe de placement.

Partager un groupe de placement

Le partage de groupes de placement vous permet d'influencer le placement d'instances interdépendantes détenues par AWS des comptes distincts. Vous pouvez partager un groupe de placement entre plusieurs AWS comptes ou au sein de vos organisations. Vous pouvez lancer des instances dans un groupe de placement partagé.

Le propriétaire d'un groupe de placement peut partager un groupe de placement avec :

- AWS Comptes spécifiques à l'intérieur ou à l'extérieur de son organisation
- Une unité d'organisation dans son organisation
- L'ensemble de son organisation

Note

Le AWS compte à partir duquel vous souhaitez partager un groupe de placement doit disposer des autorisations suivantes dans la politique IAM.

- `ec2:PutResourcePolicy`
- `ec2>DeleteResourcePolicy`

Rubriques

- [Règles et limitations](#)
- [Partager sur plusieurs zones de disponibilité](#)
- [Partager un groupe de placement](#)
- [Identifier un groupe de placement partagé](#)
- [Lancer une instance dans un groupe de placement partagé](#)
- [Annuler le partage d'un groupe de placement partagé](#)

Règles et limitations

Les règles et restrictions suivantes s'appliquent lorsque vous partagez un groupe de placement ou lorsqu'un groupe de placement est partagé avec vous.

- Pour partager un groupe de placement, vous devez en être le propriétaire dans votre AWS compte. Vous ne pouvez pas partager un groupe de placement qui a été partagé avec vous.
- Lorsque vous partagez un groupe de placement de partitions ou un groupe de placement étendu, les limites des groupes de placement ne changent pas. Un groupe de placement de partitions prend en charge un maximum de sept partitions par zone de disponibilité, tandis qu'un groupe de placement étendu prend en charge un maximum de sept instances en cours d'exécution par zone de disponibilité.
- Pour partager un groupe de placement avec votre organisation ou une unité organisationnelle de votre organisation, vous devez activer le partage avec AWS Organizations. Pour plus d'informations, consultez [Partage de vos ressources AWS](#).
- Vous êtes responsable de la gestion des instances que vous possédez dans un groupe de placement partagé.
- Vous ne pouvez pas afficher ni modifier les instances et les réserves de capacité qui sont associées à un groupe de placement partagé, mais qui ne vous appartiennent pas.

Partager sur plusieurs zones de disponibilité

Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte. Cela peut entraîner des différences de nom de zone de disponibilité entre les comptes. Par exemple, il est possible que la zone us-east-1a de disponibilité de votre AWS compte ne soit pas la même que celle us-east-1a d'un autre AWS compte.

Pour identifier l'emplacement de vos Hôtes dédiés par rapport à vos comptes, vous devez utiliser l'ID de zone de disponibilité. L'ID de zone de disponibilité est un identifiant unique et cohérent pour une zone de disponibilité entre tous les comptes AWS . Par exemple, use1-az1 est un ID de zone de disponibilité pour la région us-east-1, qui correspond au même emplacement dans chaque compte AWS .

Pour afficher les ID des zones de disponibilité dans votre compte

1. Ouvrez la AWS RAM console à l'[adresse https://console.aws.amazon.com/ram](https://console.aws.amazon.com/ram).
2. Les ID de zone de disponibilité pour la région actuelle sont affichés sous Your AZ ID (Votre ID de zone de disponibilité) dans le volet de droite.

Partager un groupe de placement

Pour partager un groupe de placement, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une AWS RAM ressource qui vous permet de partager vos ressources entre différents AWS comptes. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées.

Si vous faites partie d'une organisation et que le AWS Organizations partage au sein de votre organisation est activé, les clients de votre organisation ont accès au groupe de placement partagé.

Si le groupe de placement est partagé avec un AWS compte extérieur à votre organisation, le propriétaire du AWS compte recevra une invitation à rejoindre le partage des ressources. Ils peuvent accéder au groupe de placement partagé après avoir accepté l'invitation.

Vous pouvez partager un groupe de placement sur plusieurs AWS comptes à l'aide de <https://console.aws.amazon.com/ram> ou AWS CLI.

AWS RAM console

Pour partager un groupe de placement qui vous appartient à l'aide de <https://console.aws.amazon.com/ram>, veuillez consulter [Création d'un partage de ressources](#).

AWS CLI

Pour partager un groupe de placement dont vous êtes le propriétaire, utilisez la commande [create-resource-share](#).

Identifier un groupe de placement partagé

L'Amazon Resource Name (ARN) d'un groupe de placement contient l'ID de compte à 12 chiffres du compte propriétaire du groupe de placement. Vous pouvez utiliser l'identifiant du compte pour identifier le propriétaire d'un groupe de placement partagé avec vous.

Vous pouvez trouver l'ARN du groupe de placement à l'aide de l'une des méthodes suivantes. Pour plus d'informations, consultez [Afficher les informations sur le groupe de placement](#).

Amazon EC2 console

Pour identifier un groupe de placement partagé

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Réseau et sécurité, choisissez Placement Groups.
3. Le tableau Groupes de placement répertorie tous les groupes de placement qui vous appartiennent et que vous partagez avec vous. La colonne ARN du groupe affiche l'ARN du groupe de placement.

Si la colonne ARN du groupe n'est pas visible, choisissez settings



) dans le coin supérieur droit, activez l'ARN du groupe et choisissez Confirmer.

AWS CLI

Pour identifier un groupe de placement partagé

Utilisez [describe-placement-groups](#) la commande pour répertorier tous les groupes de placement qui vous appartiennent et qui sont partagés avec vous. Dans la réponse, le GroupId paramètre affiche l'ARN d'un groupe de placement.

Lancer une instance dans un groupe de placement partagé

Important

Lorsque vous utilisez le AWS CLI pour lancer une instance dans un groupe de placement partagé, vous devez spécifier l'ID du groupe de placement à l'aide du GroupId paramètre.

Vous ne pouvez utiliser le nom du groupe de placement que si vous êtes le propriétaire du groupe de placement partagé. Nous vous recommandons d'utiliser l'identifiant du groupe de placement pour éviter d'éventuelles collisions entre les noms des groupes de placement entre les AWS comptes.

Vous pouvez trouver l'ID d'un groupe de placement dans la console Amazon EC2 sur l'écran Groupes de placement ou à l'aide de la [describe-placement-groups](#) AWS CLI commande. Pour plus d'informations, consultez [Afficher les informations sur le groupe de placement](#).

Console

Pour lancer des instances dans un groupe de placement partagé

1. Suivez la procédure pour [lancer une instance](#), mais ne lancez pas l'instance tant que vous n'avez pas effectué les étapes suivantes pour spécifier les paramètres du groupe de placement.
2. Pour Instance type (Type d'Instance), sélectionnez un type d'instance pris en charge. Pour plus d'informations, consultez [Règles et restrictions des groupes de placement](#).
3. Développez les détails avancés et configurez les paramètres du groupe de placement comme suit :
 - a. Pour Groupe de placement, sélectionnez le groupe de placement qui a été partagé avec vous.

Note

S'il existe des groupes de placement portant le même nom, vérifiez l'ID du groupe de placement pour vous assurer que vous avez sélectionné le bon groupe de placement.

- b. Si vous choisissez un groupe de placement avec une stratégie de partition, pour Partition cible, choisissez la partition dans laquelle lancer l'instance.
4. Dans le panneau Résumé, procédez comme suit :
 - a. Pour le Number of instances (Nombre d'instances), saisissez le nombre total d'instances dont vous aurez besoin dans le groupe de placement, car vous ne pourrez peut-être pas ajouter des instances ultérieurement dans celui-ci.
 - b. Vérifiez la configuration de votre instance, puis choisissez Launch instance.

Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

AWS CLI

Pour lancer des instance dans un groupe de placement partagé

Utilisez la [run-instances](#) commande et spécifiez l'ID du groupe de placement partagé.

```
aws ec2 run-instances --placement "GroupId = pg-0123456789example"
```

Pour lancer des instances d'une partition donnée d'un groupe de placement de partitions

Utilisez la [run-instances](#) commande et spécifiez l'ID du groupe de placement et le numéro de partition du groupe de placement partagé.

```
aws ec2 run-instances --placement "GroupId = pg-0123456789example, PartitionNumber = 3"
```

Tip

Utilisez le peering VPC pour connecter des instances détenues par des AWS comptes distincts et bénéficier de tous les avantages de latence offerts par les groupes de placement de clusters partagés. Pour plus d'informations, veuillez consulter [Qu'est-ce que l'appairage de VPC ?](#)

Annuler le partage d'un groupe de placement partagé

Le propriétaire du groupe de placement peut annuler le partage d'un groupe de placement partagé à tout moment.

Lorsque vous annulez le partage d'un groupe de placement partagé, les modifications suivantes prennent effet.

- Les AWS comptes avec lesquels un groupe de placement a été partagé ne pourront plus lancer d'instances ni réserver de capacité.
- Si vos instances s'exécutaient dans un groupe de placement partagé, elles seront dissociées du groupe de placement, mais continueront à fonctionner normalement dans votre compte AWS .

- Si vous avez réservé des places dans un groupe de placement partagé, celles-ci seront dissociées du groupe de placement, mais vous continuerez d'y avoir accès dans votre AWS compte.

Vous pouvez annuler le partage d'un groupe de placement partagé en employant l'une des méthodes suivantes.

AWS RAM console

Pour annuler le partage d'un groupe de placement partagé à l'aide de <https://console.aws.amazon.com/ram>, consultez [Supprimer un partage de ressources](#).

AWS CLI

Pour annuler le partage d'un groupe de placement partagé à l'aide de AWS Command Line Interface, utilisez la commande [disassociate-resource-share](#).

Groupes de placement sur AWS Outposts

AWS Outposts est un service entièrement géré qui étend AWS l'infrastructure, les services, les API et les outils aux locaux des clients. En fournissant un accès local à l'infrastructure AWS gérée, il AWS Outposts permet aux clients de créer et d'exécuter des applications sur site en utilisant les mêmes interfaces de programmation que dans AWS les régions, tout en utilisant les ressources de calcul et de stockage locales pour réduire la latence et les besoins de traitement des données locaux.

Un avant-poste est un pool de capacités de AWS calcul et de stockage déployé sur le site d'un client. AWS exploite, surveille et gère cette capacité dans le cadre d'une AWS région.

Vous pouvez créer des groupes de placement sur les Outposts que vous avez créés dans votre compte. Cela vous permet de répartir les instances sur le matériel sous-jacent d'un Outpost sur votre site. Vous créez et utilisez les groupes de placement sur les Outposts de la même manière que vous créez et utilisez les groupes de placement dans les zones de disponibilité ordinaires. Lorsque vous créez un groupe de placement avec une stratégie de répartition sur un Outpost, vous pouvez choisir que le groupe de placement répartisse les instances sur des hôtes ou des racks. La répartition des instances entre les hôtes vous permet d'utiliser une stratégie de répartition avec un Outpost à rack unique.

Considérations

- Un groupe de placement de spread au niveau du rack peut contenir autant d'instances que vous avez de racks dans votre déploiement Outpost.

- Un groupe de placement de spread au niveau de l'hôte peut contenir autant d'instances que d'hôtes dans votre déploiement Outpost.

Prérequis

Vous devez avoir un outpost installé sur votre site. Pour plus d'informations, consultez [Créer un outpost et commander une capacité outpost](#) dans le Guide de l'utilisateur AWS Outposts .

Pour utiliser un groupe de placement sur un Outpost

1. Créez un sous-réseau sur l'outpost. Pour plus d'informations, consultez [Créer un sous-réseau](#) dans le Guide de l'utilisateur AWS Outposts .
2. Créez un groupe de placement dans la région associée de l'Outpost. Si vous créez un groupe de placement avec une stratégie de spread, vous pouvez choisir un spread au niveau de l'hôte ou du rack pour déterminer comment le groupe répartira les instances sur le matériel sous-jacent de votre Outpost. Pour plus d'informations, consultez [the section called "Créer un groupe de placement."](#)
3. Lancez une instance dans le groupe de placement. Pour Subnet (Sous-réseau), choisissez le sous-réseau que vous avez créé à l'étape 1. Pour Placement group name (Nom du groupe de placement), sélectionnez le groupe de placement que vous avez créé à l'étape 2. Pour plus d'informations, consultez la section [Lancer une instance sur votre Outpost](#) du Guide de l'utilisateur AWS Outposts .

Unité de transmission maximale (MTU) du réseau pour votre instance EC2

L'unité de transmission maximale (MTU) d'une connexion réseau correspond à la taille, en octets, du paquet le plus volumineux susceptible d'être transmis via la connexion. Plus la MTU d'une connexion est élevée, plus la quantité de données pouvant être transmises dans un seul paquet est importante. Les trames Ethernet se composent du paquet, ou des données réelles que vous envoyez, et des informations de surcharge du réseau qui l'entourent.

Les trames Ethernet peuvent avoir différents formats, le plus courant étant le format de trame standard Ethernet v2. Il prend en charge une MTU de 1500, c'est-à-dire la taille de paquet Ethernet la plus importante prise en charge presque partout sur Internet. La MTU maximum prise en charge pour une instance dépend du type d'instance.

Les règles suivantes s'appliquent aux instances qui se trouvent dans des zones Wavelength :

- Le trafic qui passe d'une instance à une autre au sein d'un VPC dans la même zone Wavelength a un MTU de 1300.
- Le trafic qui passe d'une instance à une autre qui utilise l'adresse IP du transporteur dans une zone Wavelength a une MTU de 1500.
- Le trafic qui passe d'une instance à une autre entre une zone Wavelength et une région qui utilise une adresse IP publique a une MTU de 1500.
- Le trafic qui passe d'une instance à une autre entre une zone Wavelength et une région qui utilise une adresse IP privée a une MTU de 1300.

Les règles suivantes s'appliquent aux instances qui se trouvent dans Outposts :

- Le trafic qui passe d'une instance dans Outposts à une instance dans la région a un MTU de 1 300.

Table des matières

- [Trames jumbo \(MTU de 9001\)](#)
- [Détection de la MTU du chemin](#)
- [Vérifier la MTU du chemin entre deux hôtes](#)
- [Vérifiez le MTU de votre instance](#)
- [Définissez le MTU pour votre instance](#)
- [Dépannage](#)

Trames jumbo (MTU de 9001)

Les trames jumbo permettent d'utiliser plus de 1 500 octets de données en augmentant la charge utile par paquet, et donc en augmentant le pourcentage de paquet qui ne constitue pas des frais supplémentaires. Moins de paquets sont nécessaires pour envoyer le même volume de données utilisables. Toutefois, le trafic est limité à une MTU maximale de 1 500 dans les cas suivants :

- Trafic sur une passerelle Internet
- Trafic sur une connexion d'appairage de VPC entre régions
- Trafic sur des connexions VPN
- Trafic en dehors d'une AWS région donnée

Si la taille des paquets dépasse 1 500 octets, ceux-ci sont fragmentés ou abandonnés si l'indicateur `Don't Fragment` est défini dans l'en-tête IP.

Les trames jumbo doivent être utilisées avec prudence pour le trafic Internet ou pour tout trafic quittant un VPC. Les paquets sont fragmentés par des systèmes intermédiaires, ce qui ralentit le trafic. Pour utiliser les trames jumbo dans un VPC et éviter de ralentir le trafic destiné à sortir du VPC, vous pouvez configurer la taille de MTU par routage ou utiliser plusieurs interfaces réseau Elastic avec différentes tailles de MTU et différents routages.

Pour les instances situées dans un même groupe de placement du cluster, les trames jumbo permettent d'atteindre le débit réseau maximum possible et elles sont recommandées dans ce cas. Pour plus d'informations, consultez [Groupes de placement](#).

Vous pouvez utiliser des trames jumbo pour le trafic entre vos VPC et vos réseaux sur site via AWS Direct Connect. Pour plus d'informations et pour savoir comment vérifier la capacité de trame Jumbo, consultez [Configuration de la MTU du réseau](#) dans le AWS Direct Connect Guide de l'utilisateur.

Tous les types d'instances Amazon EC2 prennent en charge 1 500 MTU et tous les types d'instances de la génération actuelle prennent en charge les trames jumbo. Les types d'instances de la génération précédente suivants prennent en charge les trames jumbo : A1, C3, I2, M3 et R3.

Pour plus d'informations sur les tailles d'AMI prises en charge :

- Pour les passerelles NAT, consultez la section [Principe de base d'une passerelle NAT](#) dans le Guide de l'utilisateur Amazon VPC.
- Pour les passerelles de transit, veuillez consulter [MTU](#) dans le Guide de l'utilisateur Amazon VPC Transit Gateways.
- Pour les zones locales, consultez la section [Considérations](#) dans le Guide de l'utilisateur des zones locales AWS .

Détection de la MTU du chemin

La détection de la MTU du chemin (PMTUD) permet de déterminer la MTU du chemin entre deux appareils. La MTU du chemin correspond à la taille maximum du paquet prise en charge sur le chemin entre l'hôte de départ et l'hôte de destination. En cas de différence de taille de la MTU sur le réseau entre deux hôtes, la PMTUD permet à l'hôte de réception de répondre à l'hôte d'origine avec un message ICMP. Ce message ICMP indique que l'hôte d'origine utilise la taille de MTU la plus petite sur chemin d'accès réseau pour renvoyer la demande. Sans cette négociation, un rejet de paquet peut se produire, car la demande est trop volumineuse pour l'hôte de réception.

Pour IPv4, si un hôte envoie un paquet dont la taille est plus importante que la MTU définie pour l'hôte destinataire ou que celle d'un appareil se trouvant sur le chemin, l'hôte ou l'appareil destinataire supprime le paquet et retourne le message ICMP suivant : `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set (Type 3, Code 4)`. Cela indique à l'hôte émetteur de diviser la charge utile en plusieurs paquets plus petits, puis de les retransmettre.

Le protocole IPv6 ne prend pas en charge la fragmentation dans le réseau. Si un hôte envoie un paquet dont la taille est plus importante que la MTU définie pour l'hôte destinataire ou que celle d'un appareil se trouvant sur le chemin, l'hôte ou l'appareil destinataire supprime le paquet et retourne le message ICMP suivant : `ICMPv6 Packet Too Big (PTB) (Type 2)`. Cela indique à l'hôte émetteur de diviser la charge utile en plusieurs paquets plus petits, puis de les retransmettre.

Les connexions établies via certains composants, tels que les passerelles NAT et les équilibreurs de charge, font l'objet d'un [suivi automatique](#). Cela signifie que le [suivi des groupes de sécurité](#) est automatiquement activé pour vos tentatives de connexion sortante. Si les connexions font l'objet d'un suivi automatique ou si les règles de votre groupe de sécurité autorisent le trafic ICMP entrant, vous pouvez recevoir des réponses PMTUD.

Notez que le trafic ICMP peut être bloqué même s'il est autorisé au niveau du groupe de sécurité, par exemple si une entrée de la liste de contrôle d'accès réseau refuse le trafic ICMP vers le sous-réseau.

Important

Path MTU Discovery ne garantit pas que les trames jumbo ne seront pas abandonnées par certains routeurs. Une passerelle Internet sur votre VPC transmettra uniquement les paquets de 1 500 octets au maximum. Les paquets dont la MTU est de 1500 sont recommandés pour le trafic Internet.

Vérifier la MTU du chemin entre deux hôtes

Vous pouvez vérifier le chemin MTU entre votre instance EC2 et un autre hôte. Vous pouvez spécifier un nom DNS ou une adresse IP comme destination. Si la destination est une autre instance EC2, vérifiez que son groupe de sécurité autorise le trafic UDP entrant.

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Instances Linux

Exécutez la `tracert` commande sur votre instance pour vérifier le chemin MTU entre votre instance EC2 et la destination spécifiée. Cette commande fait partie du `iputils` package, qui est disponible par défaut dans de nombreuses distributions Linux.

Cet exemple vérifie le chemin MTU entre l'instance EC2 et `amazon.com`

```
[ec2-user ~]$ tracepath amazon.com
```

Dans cet exemple de sortie, le chemin MTU est 1500.

```
1?: [LOCALHOST]      pmtu 9001
1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)    0.187ms pmtu 1500
1:  no reply
2:  no reply
3:  no reply
4:  100.64.16.241 (100.64.16.241)                0.574ms
5:  72.21.222.221 (72.21.222.221)                84.447ms asymm 21
6:  205.251.229.97 (205.251.229.97)             79.970ms asymm 19
7:  72.21.222.194 (72.21.222.194)              96.546ms asymm 16
8:  72.21.222.239 (72.21.222.239)              79.244ms asymm 15
9:  205.251.225.73 (205.251.225.73)            91.867ms asymm 16
...
31: no reply
    Too many hops: pmtu 1500
    Resume: pmtu 1500
```

instances Windows

Pour vérifier le MTU du chemin à l'aide de `mturoute`

1. Téléchargez `mturoute.exe` sur votre instance EC2 depuis <http://www.elifulkerson.com/projects/mturoute.php>.
2. Ouvrez une fenêtre d'invite de commande et modifiez l'annuaire dans lequel vous avez téléchargé `mturoute.exe`.
3. Utilisez la commande suivante pour vérifier le chemin MTU entre votre instance EC2 et la destination spécifiée. Cet exemple vérifie le chemin MTU entre l'instance EC2 et `www.elifulkerson.com`

```
.\mturoute.exe www.elifulkerson.com
```

Dans cet exemple de sortie, le chemin MTU est 1500.

```
* ICMP Fragmentation is not permitted. *
* Speed optimization is enabled. *
* Maximum payload is 10000 bytes. *
+ ICMP payload of 1472 bytes succeeded.
- ICMP payload of 1473 bytes is too big.
Path MTU: 1500 bytes.
```

Vérifiez le MTU de votre instance

Vous pouvez vérifier la valeur MTU de votre instance. Certaines instances sont configurées de façon à utiliser les trames jumbo, tandis que d'autres sont configurées de façon à utiliser les tailles de trame standard.

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Instances Linux

Pour vérifier le paramètre MTU sur une instance Linux

Exécutez la ip commande suivante sur votre instance EC2. Si ce n'est pas le cas de l'interface réseau principale eth0, eth0 remplacez-la par votre interface réseau.

```
[ec2-user ~]$ ip link show eth0
```

Dans cet exemple de sortie, *mtu 9001* indique que l'instance utilise des trames jumbo.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
  DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

instances Windows

La procédure que vous utilisez dépend du pilote de votre instance.

ENA driver

Version 2.1.0 et versions ultérieures

Pour obtenir la valeur MTU, utilisez la `Get-NetAdapterAdvancedProperty` commande suivante sur votre instance EC2. Utilisez le caractère générique (astérisque) pour obtenir tous les noms Ethernet. Vérifiez la sortie pour le nom de l'interface* `JumboPacket`. La valeur 9015 indique que les trames Jumbo sont activées. Les trames Jumbo sont désactivées par défaut.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Version 1.5 et antérieures

Pour obtenir la valeur MTU, utilisez la `Get-NetAdapterAdvancedProperty` commande suivante sur votre instance EC2. Vérifiez la sortie pour le nom de l'interface `MTU`. La valeur 9001 indique que les trames Jumbo sont activées. Les trames Jumbo sont désactivées par défaut.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Pour obtenir la valeur MTU, utilisez la `Get-NetAdapterAdvancedProperty` commande suivante sur votre instance EC2. Vérifiez l'entrée pour le nom d'interface * `JumboPacket`. La valeur 9014 indique que les trames Jumbo sont activées. (Notez que la taille MTU inclut l'en-tête et la charge utile.) Les trames Jumbo sont désactivées par défaut.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Pour obtenir la valeur MTU, utilisez la commande suivante sur votre instance EC2. Le nom de l'interface peut varier. Dans la sortie, recherchez une entrée portant le nom « Ethernet », « Ethernet 2 » ou « Local Area Connection ». Vous aurez besoin du nom d'interface pour activer ou désactiver les trames Jumbo. La valeur 9001 indique que les trames Jumbo sont activées.

```
netsh interface ipv4 show subinterface
```

Définissez le MTU pour votre instance

Vous souhaitez peut-être utiliser des trames jumbo pour le trafic réseau au sein de votre VPC et des trames standard pour le trafic Internet. Quel que soit votre cas d'utilisation, nous vous recommandons de vérifier que votre instance se comporte comme prévu.

La procédure que vous utilisez dépend du système d'exploitation de l'instance.

Instances Linux

Pour définir la valeur de la MTU sur une instance Linux

1. Exécutez la `ip` commande suivante sur votre instance. Il définit la valeur MTU souhaitée sur 1500, mais vous pouvez utiliser 9001 à la place.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
```

2. (Facultatif) Pour conserver le paramètre de la MTU du réseau après le redémarrage, modifiez les fichiers de configuration suivants en fonction de votre type de système d'exploitation.
 - Pour Amazon Linux 2, ajoutez la ligne suivante au fichier `/etc/sysconfig/network-scripts/ifcfg-eth0`:

```
MTU=1500
```

Ajoutez la ligne suivante dans le fichier `/etc/dhcp/dhclient.conf` :

```
request subnet-mask, broadcast-address, time-offset, routers, domain-name,  
domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-  
servers;
```

- Pour l'AMI Amazon Linux, ajoutez les lignes suivantes à votre `/etc/dhcp/dhclient-eth0.conf` fichier.

```
interface "eth0" {  
supersede interface-mtu 1500;  
}
```

- Pour les autres distributions Linux, consultez leur documentation spécifique.
3. (Facultatif) Redémarrez l'instance et vérifiez que le paramètre MTU est correct.

instances Windows

La procédure que vous utilisez dépend du pilote de votre instance.

ENA driver

Vous pouvez modifier le MTU à l'aide du Gestionnaire de périphériques ou de la `Set-NetAdapterAdvancedProperty` commande de votre instance.

Version 2.1.0 et versions ultérieures

Utilisez la commande suivante pour activer les cadres jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -RegistryValue 9015
```

Utilisez la commande suivante pour désactiver les images jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -RegistryValue 1514
```

Version 1.5 et antérieures

Utilisez la commande suivante pour activer les cadres jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -RegistryValue 9001
```

Utilisez la commande suivante pour désactiver les images jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -RegistryValue 1500
```

Intel SRIOV 82599 driver

Vous pouvez modifier le MTU à l'aide du Gestionnaire de périphériques ou de la `Set-NetAdapterAdvancedProperty` commande de votre instance.

Utilisez la commande suivante pour activer les cadres jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -RegistryValue 9014
```

Utilisez la commande suivante pour désactiver les images jumbo.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -RegistryValue 1514
```

AWS PV driver

Vous pouvez modifier le MTU à l'aide de la netsh commande de votre instance. Vous ne pouvez pas modifier le MTU à l'aide du Gestionnaire de périphériques.

Utilisez la commande suivante pour activer les cadres jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Utilisez la commande suivante pour désactiver les images jumbo.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Dépannage

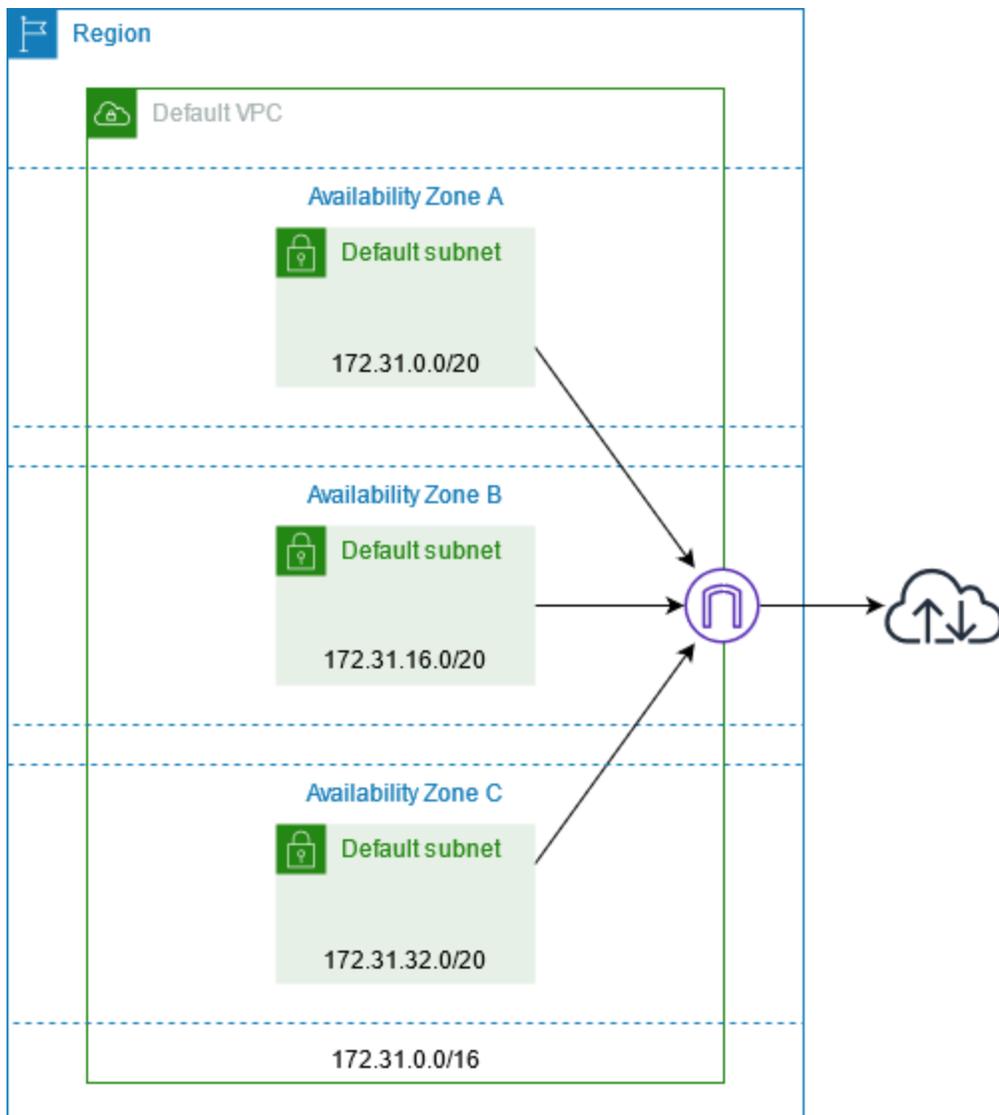
Si vous rencontrez des problèmes de connectivité entre votre instance EC2 et un cluster Amazon Redshift lorsque vous utilisez des trames jumbo, [consultez la section Queries Appear to Hang](#) dans le guide de gestion Amazon Redshift.

Clouds privés virtuels pour vos instances EC2

Amazon Virtual Private Cloud (Amazon VPC) vous permet de définir un réseau virtuel dans votre propre zone logiquement isolée au sein du AWS cloud, connu sous le nom de cloud privé virtuel ou VPC. Vous pouvez créer des AWS ressources, telles que des instances Amazon EC2, dans les sous-réseaux de votre VPC. Votre VPC ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données, et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS. Vous pouvez configurer votre VPC en sélectionnant sa plage d'adresses IP, en créant des sous-réseaux et en configurant des tables de routage, des passerelles réseau et des paramètres de sécurité. Vous pouvez connecter des instances dans votre VPC à Internet ou à votre propre centre de données.

Vos VPC par défaut

Lorsque vous créez votre AWS compte, nous créons un VPC par défaut dans chaque région. Un VPC par défaut est un VPC déjà configuré et prêt à être utilisé par vous. Par exemple, il existe un sous-réseau par défaut pour chaque zone de disponibilité dans chaque VPC par défaut, une passerelle Internet reliée au VPC et la table de routage principale contient un acheminement qui envoie tout le trafic (0.0.0.0/0) à la passerelle Internet. Vous pouvez également créer votre propre VPC et le configurer en fonction de vos besoins.



Création de VPC supplémentaires

Utilisez la procédure suivante pour créer un VPC avec les sous-réseaux, les passerelles et la configuration de routage dont vous avez besoin.

Pour créer un VPC

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Sélectionnez Create VPC (Créer un VPC).
3. Sous Resources to create (Ressources à créer), choisissez VPC and more (VPC et autres).
4. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.
5. Pour le bloc CIDR IPv4, conservez la suggestion par défaut ou saisissez le bloc CIDR requis par votre application ou votre réseau.
6. Pour Number of Availability Zones (Nombre de zones de disponibilité), choisissez 2, afin de pouvoir lancer des instances dans plusieurs zones de disponibilité et assurer ainsi une haute disponibilité.
7. Si vos instances doivent être accessibles depuis Internet, effectuez l'une des actions suivantes :
 - Si vos instances peuvent se trouver dans un sous-réseau public, sélectionnez une valeur non nulle pour Number of public subnets (Nombre de sous-réseaux publics). Conservez les deux options sous les options DNS sélectionnées. Vous pouvez éventuellement ajouter des sous-réseaux privés maintenant ou ultérieurement.
 - Si vos instances doivent être dans un sous-réseau privé, sélectionnez 0 pour Number of public subnets (Nombre de sous-réseaux publics). Pour Number of private subnets (Nombre de sous-réseaux privés), sélectionnez un nombre en fonction de vos besoins (les valeurs possibles correspondent à 1 ou 2 sous-réseaux privés par zone de disponibilité). Pour les NAT gateways (Passerelles NAT), si vos instances dans les deux zones de disponibilité envoient ou reçoivent un volume important de trafic à travers les zones de disponibilité, sélectionnez 1 per AZ (1 par zone de disponibilité). Sinon, sélectionnez In 1 AZ (Dans une zone de disponibilité) et lancez des instances qui envoient ou reçoivent du trafic entre zones dans la même zone de disponibilité que la passerelle NAT.
8. Développez Customize subnet CIDR blocks (Personnaliser les blocs CIDR du sous-réseau). Conservez les suggestions par défaut ou saisissez un bloc CIDR pour chaque sous-réseau. Pour plus d'informations, consultez [Blocs d'adresse CIDR de sous-réseau](#) dans le Guide de l'utilisateur Amazon VPC.
9. Consultez le volet Preview (Aperçu), qui affiche les ressources VPC qui seront créées en fonction de vos sélections.
10. Sélectionnez Create VPC (Créer un VPC).

Accès à Internet depuis vos instances

Les instances lancées dans un sous-réseau par défaut d'un VPC par défaut ont accès à Internet, car les VPC par défaut sont configurés pour attribuer des adresses IP publiques et des noms d'hôte DNS, et la table de routage principale est configurée avec une route vers une passerelle Internet attachée au VPC.

Pour les instances que vous lancez dans des sous-réseaux et des VPC autres que ceux par défaut, vous pouvez utiliser l'une des options suivantes pour vous assurer que les instances que vous lancez dans ces sous-réseaux ont accès à Internet :

- Configurez une passerelle Internet. Pour plus d'informations, consultez [Connexion à l'Internet à l'aide d'une passerelle Internet](#) dans le Guide de l'utilisateur Amazon VPC.
- Configurez une passerelle NAT publique. Pour plus d'informations, consultez [Accéder à Internet à partir d'un sous-réseau privé](#) dans le Guide de l'utilisateur Amazon VPC.

Sous-réseaux partagés

Lorsque vous lancez des instances EC2 dans des sous-réseaux VPC partagés, tenez compte des points suivants :

- Les participants peuvent exécuter des instances dans un sous-réseau partagé en spécifiant l'ID du sous-réseau partagé. Les participants doivent posséder les groupes de sécurité ou les interfaces réseau qu'ils spécifient.
- Les participants peuvent démarrer, arrêter, terminer et décrire les instances qu'ils ont créées dans un sous-réseau partagé. Les participants ne peuvent pas démarrer, arrêter, terminer ou décrire les instances créées par le propriétaire du VPC dans le sous-réseau partagé.
- Les propriétaires de VPC ne peuvent pas démarrer, arrêter, terminer ou décrire les instances créées par les participants dans un sous-réseau partagé.
- Les participants peuvent se connecter à une instance dans un sous-réseau partagé à l'aide du point de terminaison EC2 Instance Connect. Le participant doit créer le point de terminaison EC2 Instance Connect dans le sous-réseau partagé. Les participants ne peuvent pas utiliser un point de terminaison EC2 Instance Connect créé par le propriétaire du VPC dans le sous-réseau partagé.

Pour plus d'informations, consultez [Partager votre VPC avec d'autres comptes](#) dans le Guide de l'utilisateur Amazon VPC.

Sous-réseaux IPv6 uniquement

Une instance EC2 lancée dans un sous-réseau IPv6 uniquement reçoit une adresse IPv6 mais pas d'adresse IPv4. Toutes les instances que vous lancez dans un sous-réseau IPv6 uniquement doivent être des [instances créées sur le](#) système Nitro. AWS

Sécurité dans Amazon EC2

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le [modèle de responsabilité partagée](#) décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de [AWS conformité Programmes](#) de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon EC2, consultez [AWS Services concernés par programme de conformité AWS Services couverts par programme](#) .
- Sécurité dans le cloud : votre responsabilité englobe les domaines suivants :
 - Contrôler l'accès réseau à vos instances, par exemple, en configurant votre VPC et vos groupes de sécurité. Pour plus d'informations, consultez [Contrôle du trafic réseau](#).
 - Gestion des informations d'identification utilisées pour vous connecter à vos instances.
 - Gestion du système d'exploitation invité et des logiciels déployés sur le système d'exploitation invité, y compris les mises à jour et les correctifs de sécurité. Pour plus d'informations, consultez [Gestion des mises à jour pour les instances Windows Amazon EC2](#).
 - Configuration des rôles IAM attachés à l'instance et des autorisations associées à ces rôles. Pour plus d'informations, consultez [Rôles IAM pour Amazon EC2](#).

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Amazon EC2. Elle vous montre comment configurer Amazon EC2 pour atteindre vos objectifs en matière de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Amazon EC2.

Table des matières

- [Protection des données dans Amazon EC2](#)
- [Sécurité de l'infrastructure dans Amazon EC2](#)
- [Résilience dans Amazon EC2](#)

- [Validation de la conformité pour Amazon EC2](#)
- [Identity and Access Management pour Amazon EC2](#)
- [Accéder à Amazon EC2 à l'aide du point de terminaison d'un VPC d'interface](#)
- [Gestion des mises à jour pour les instances Windows Amazon EC2](#)
- [Bonnes pratiques de sécurité pour les instances Windows](#)
- [Paires de clés Amazon EC2 et instances Amazon EC2](#)
- [Groupes de sécurité Amazon EC2 pour vos instances EC2](#)
- [NitroTPM](#)
- [Credential Guard pour les instances Windows](#)

Protection des données dans Amazon EC2

Le [modèle de responsabilité AWS partagée](#) s'applique à la protection des données dans Amazon Elastic Compute Cloud. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez [Questions fréquentes \(FAQ\) sur la confidentialité des données](#). Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog [Modèle de responsabilité partagée AWS et RGPD \(Règlement général sur la protection des données\)](#) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.

- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez [Federal Information Processing Standard \(FIPS\) 140-2](#) (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Amazon EC2 ou une autre entreprise à Services AWS l'aide de la console, de l'API ou AWS des AWS CLI SDK. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Table des matières

- [Sécurité des données Amazon EBS](#)
- [Chiffrement au repos](#)
- [Chiffrement en transit](#)

Sécurité des données Amazon EBS

Les volumes Amazon EBS vous sont présentés comme des périphériques de stockage en mode bloc bruts non formatés. Ces appareils sont des périphériques logiques créés sur l'infrastructure EBS et le service Amazon EBS garantit que les appareils sont logiquement vides (c'est-à-dire que les blocs bruts sont mis à zéro ou contiennent des données pseudo-aléatoires cryptographiques) avant toute utilisation ou réutilisation par un client.

Si vous avez des procédures qui exigent que toutes les données soient effacées à l'aide d'une méthode spécifique, après ou avant utilisation (ou les deux), telles que celles détaillées dans DoD 5220.22-M (National Industrial Security Program Operating Manual) ou NIST 800-88 (Guidelines for Media Sanitization), vous avez la possibilité de le faire sur Amazon EBS. Cette activité de niveau bloc sera reflétée sur le support de stockage sous-jacent du service Amazon EBS.

Chiffrement au repos

Volumes EBS

Le chiffrement Amazon EBS est une solution de chiffrement destinées à vos volumes et instantanés EBS. Il utilise AWS KMS keys. Pour plus d'informations, consultez la section relative au [chiffrement Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

[Instances Windows] Vous pouvez également utiliser les autorisations Microsoft EFS et NTFS pour le chiffrement au niveau des dossiers et des fichiers.

Volumes de stockage d'instances

Les données sur les volumes de stockage d'instance NVMe sont chiffrées à l'aide d'un chiffrement XTS-AES-256 implémenté dans un module matériel sur l'instance. Les clés utilisées pour chiffrer les données écrites sur des périphériques de stockage NVMe connectés localement sont par client et par volume. Les clés sont générées par le module matériel et ne se trouvent qu'à l'intérieur de celui-ci, qui est inaccessible au personnel AWS . Les clés de chiffrement sont détruites lorsque l'instance est arrêtée ou résiliée et ne peuvent pas être récupérées. Vous ne pouvez pas désactiver le chiffrement et vous ne pouvez pas fournir votre propre clé de chiffrement.

Les données sur des volumes de stockage d'instance HDD sur des instances H1, D3 et D3en sont chiffrées à l'aide de clés XTS-AES-256 et de clés uniques.

Lorsque vous arrêtez, mettez en veille prolongée ou résiliez une instance, chaque bloc de stockage du volume de stockage d'instances est réinitialisé. Par conséquent, vos données ne sont pas accessibles via le stockage d'instances d'une autre instance.

Mémoire

Le chiffrement de la mémoire est activé sur les instances suivantes :

- Instances équipées de processeurs AWS Graviton. AWS Graviton2, AWS Graviton3 et Graviton3E prennent en charge le chiffrement permanent de la AWS mémoire. Les clés de chiffrement sont générées en toute sécurité dans le système hôte, elles ne quittent jamais le système hôte et sont détruites lorsque l'hôte est redémarré ou mis hors tension. Pour de plus amples informations, veuillez consulter [Processeurs AWS Graviton](#).
- Les instances dotées de processeurs Intel Xeon Scalable de 3e génération (Ice Lake), telles que les instances M6i, et de processeurs Intel Xeon Scalable de 4e génération (Sapphire Rapids), tels

que les instances M7i. Ces processeurs prennent en charge le chiffrement de mémoire permanent à l'aide d'Intel Total Memory Encryption (TME).

- Les instances dotées de processeurs AMD EPYC de 3e génération (Milan), telles que les instances M6a, et de processeurs AMD EPYC de 4e génération (Genoa), telles que les instances M7a. Ces processeurs prennent en charge le chiffrement de mémoire permanent à l'aide d'AMD Secure Memory Encryption (SME). Les instances dotées de processeurs AMD EPYC de 3e génération (Milan) prennent également en charge la technologie AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP).

Chiffrement en transit

Chiffrement au niveau de la couche physique

Toutes les données circulant entre AWS les régions via le réseau AWS mondial sont automatiquement cryptées au niveau de la couche physique avant de quitter les installations AWS sécurisées. Tout le trafic entre zones de disponibilité est chiffré. Des couches supplémentaires de chiffrement, y compris celles présentées dans cette section, peuvent fournir des protections supplémentaires.

Chiffrement fourni par le peering Amazon VPC et le peering interrégional Transit Gateway

Tout le trafic interrégional qui utilise le peering Amazon VPC et le peering Transit Gateway est automatiquement chiffré en bloc lorsqu'il quitte une région. Une couche de chiffrement supplémentaire est automatiquement fournie au niveau de la couche physique pour tout le trafic avant qu'il ne quitte les installations AWS sécurisées, comme indiqué précédemment dans cette section.

Chiffrement entre instances

AWS fournit une connectivité sécurisée et privée entre les instances EC2 de tous types. En outre, certains types d'instances utilisent les capacités de déchargement du matériel du système Nitro sous-jacent pour chiffrer automatiquement le trafic en transit entre instances. Ce chiffrement utilise des algorithmes de chiffrement authentifié avec données associées (AEAD), avec un chiffrement 256 bits. Il n'y a aucun impact sur les performances du réseau. Pour prendre en charge ce chiffrement supplémentaire du trafic en transit entre les instances, les exigences suivantes doivent être satisfaites :

- Les instances utilisent les types d'instance suivants :

- Usage général : M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7g, M7GD, M7i, M7i-Flex
- Optimisé pour le calcul : C5a, C5ad, C5n, C6a, C6gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-Flex
- Mémoire optimisée : R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7g, R7gd, R7i, R7iz, U-3tb1, U-6TB1, U-9TB1, U-24TB1, U-24TB1, U7i-12TB, U7in-16TB, U7in-16TB, U7in-16TB, U7in-16TB, U7Tb 7 en 24 To, 7 en 32 To, x2IDN, x2iEDN, x2ieZN
- Stockage optimisé : D3, D3en, i3EN, i4G, i4i, iM4GN, IS4gen
- Calcul accéléré : DL1, DL2q, G4ad, G4dn, G5, G6, Gr6, Inf1, Inf2, P3dn, P4d, P4de, P5, Trn1, TRN1n, VT1
- Calcul à hautes performances : Hpc6a, Hpc6id, Hpc7a, Hpc7g
- Les instances se trouvent dans la même région.
- Les instances se trouvent dans le même VPC ou dans des VPC appairés, et le trafic ne passe pas par un service ou un périphérique de réseau virtuel, tel qu'un équilibreur de charge ou une passerelle de transit.

Une couche de chiffrement supplémentaire est automatiquement fournie au niveau de la couche physique pour tout le trafic avant qu'il ne quitte les installations AWS sécurisées, comme indiqué précédemment dans cette section.

Pour afficher les types d'instance qui chiffrent le trafic en transit entre les instances à l'aide de la AWS CLI

Utilisez la commande [suivante de l' `describe-instance-types`](#).

```
aws ec2 describe-instance-types \
  --filters Name=network-info.encryption-in-transit-supported,Values=true \
  --query "InstanceTypes[*].[InstanceType]" \
  --output text | sort
```

Chiffrement depuis et vers AWS Outposts

Un Outpost crée des connexions réseau spéciales appelées liens de service vers sa région d'AWS origine et, éventuellement, une connectivité privée avec un sous-réseau VPC que vous spécifiez. Tout le trafic sur ces connexions est entièrement crypté. Pour plus d'informations, consultez [Connectivité via des liens de service](#) et [Chiffrement en transit](#) dans le Guide de l'utilisateur AWS Outposts .

Chiffrement d'accès distant

Les protocoles SSH et RDP fournissent des canaux de communication sécurisés pour un accès à distance à vos instances, que ce soit directement ou via EC2 Instance Connect. L'accès à distance à vos instances à l'aide du gestionnaire de AWS Systems Manager session ou de la commande Run est crypté à l'aide de TLS 1.2, et les demandes de création de connexion sont signées à l'aide de [SigV4](#), authentifiées et autorisées par [AWS Identity and Access Management](#)

Il vous incombe d'utiliser un protocole de chiffrement tel que Transport Layer Security (TLS) pour chiffrer les données sensibles en transit entre les clients et vos instances Amazon EC2.

(Instances Windows) Assurez-vous d'autoriser uniquement les connexions chiffrées entre les instances EC2 et les points de terminaison de l' AWS API ou d'autres services réseau distants sensibles. Vous pouvez mettre cela en œuvre via un groupe de sécurité sortant ou des règles du [Pare-feu Windows](#).

Sécurité de l'infrastructure dans Amazon EC2

En tant que service géré, Amazon Elastic Compute Cloud est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section [Sécurité du AWS cloud](#). Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Amazon EC2 via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser [AWS Security Token Service](#) (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Pour plus d'informations, voir [Protection de l'infrastructure](#) dans le pilier de sécurité — AWS Well-Architected Framework.

Isolement de réseau

Un cloud privé virtuel (VPC) est un réseau virtuel situé dans votre propre zone logiquement isolée dans le cloud. AWS Utilisez des VPC distincts pour isoler l'infrastructure par charge de travail ou entité organisationnelle.

Un sous-réseau est une plage d'adresses IP dans un VPC. Lorsque vous lancez une instance, vous la lancez dans un sous-réseau de votre VPC. Utilisez des sous-réseaux pour isoler les niveaux de votre application (par exemple, web, application et base de données) dans un VPC unique. Utilisez des sous-réseaux privés pour vos instances si elles ne doivent pas être accessibles directement à partir d'Internet.

Pour appeler l'API Amazon EC2 depuis votre VPC à l'aide d'adresses IP privées, utilisez AWS PrivateLink. Pour plus d'informations, consultez [Accéder à Amazon EC2 à l'aide du point de terminaison d'un VPC d'interface](#).

Isolation sur les hôtes physiques

Différentes instances EC2 sur un même hôte physique sont isolées les unes des autres comme si elles se trouvaient sur des hôtes physiques distincts. L'hyperviseur isole l'UC et la mémoire, et les instances sont équipées de disques virtuels au lieu d'accéder aux disques bruts.

Lorsque vous arrêtez ou résiliez une instance, la mémoire qui lui est allouée est remise à zéro par l'hyperviseur avant d'être allouée à une nouvelle instance, et chaque bloc de stockage est réinitialisé. Cela permet d'être sûr que vos données ne seront pas accidentellement exposées sur une autre instance.

Les adresses MAC du réseau sont attribuées dynamiquement aux instances par l'infrastructure AWS réseau. Les adresses IP sont affectées de façon dynamique aux instances par l'infrastructure réseau AWS ou affectées par un administrateur EC2 via des demandes d'API authentifiées. Le AWS réseau permet aux instances d'envoyer du trafic uniquement à partir des adresses MAC et IP qui leur sont attribuées. Dans le cas contraire, le trafic est abandonné.

Par défaut, une instance ne peut pas recevoir un trafic qui ne lui est pas spécifiquement adressé. Si vous avez besoin d'exécuter des services de translation d'adresse réseau (NAT), de routage ou de pare-feu sur votre instance, vous pouvez désactiver la vérification origine/destination pour l'interface réseau.

Contrôle du trafic réseau

Vous devez prendre en compte les éléments suivants pour le contrôle du trafic réseau vers vos instances EC2 :

- Limitez l'accès à vos instances à l'aide de [groupes de sécurité](#). Configurez des règles qui autorisent le trafic réseau minimum requis. Par exemple, vous pouvez autoriser le trafic uniquement à partir des plages d'adresses de votre réseau d'entreprise ou uniquement pour des protocoles spécifiques, tels que HTTPS. Pour les instances Windows, autorisez le trafic de gestion Windows et un minimum de connexions sortantes.
- Exploitez les groupes de sécurité comme mécanisme principal pour contrôler l'accès réseau aux instances Amazon EC2. Si nécessaire, utilisez les ACL réseau avec flottement pour fournir un contrôle de réseau sans état et à grain grossier. Les groupes de sécurité sont plus polyvalents que les ACL réseau en raison de leur capacité à effectuer un filtrage des paquets avec état et à créer des règles qui référencent d'autres groupes de sécurité. Toutefois, les ACL réseau peuvent être efficaces en tant que contrôle secondaire, pour refuser un sous-ensemble spécifique de trafic ou fournir des garde-fous de sous-réseau de haut niveau. De plus, comme les ACL réseau s'appliquent à l'ensemble d'un sous-réseau, elles peuvent être utilisées comme défense-in-depth dans le cas où une instance serait lancée par inadvertance sans un groupe de sécurité approprié.
- [Instances Windows] Gérez de manière centralisée les paramètres du pare-feu Windows avec des objets de stratégie de groupe (GPO) afin d'améliorer encore les contrôles réseau. Les clients utilisent souvent le Pare-feu Windows pour augmenter la visibilité sur le trafic réseau et pour compléter les filtres de groupe de sécurité, créant des règles avancées pour empêcher des applications spécifiques d'accéder au réseau ou pour filtrer le trafic à partir d'adresses IP d'un sous-ensemble. Par exemple, le pare-feu Windows peut limiter l'accès à l'adresse IP du service de métadonnées EC2 à des utilisateurs ou applications spécifiques. Par ailleurs, un service public peut utiliser des groupes de sécurité pour restreindre le trafic vers des ports spécifiques et le pare-feu Windows pour maintenir une liste d'adresses IP explicitement bloquées.
- Utilisez des sous-réseaux privés pour vos instances si elles ne doivent pas être accessibles directement à partir d'Internet. Utilisez un hôte bastion ou une passerelle NAT pour l'accès Internet à partir d'une instance d'un sous-réseau privé.
- [Instances Windows] Utilisez des protocoles d'administration sécurisés tels que l'encapsulation RDP via SSL/TLS. Le Quick Start de la passerelle Bureau à distance fournit les bonnes pratiques pour le déploiement de la passerelle Bureau à distance, y compris la configuration de RDP pour utiliser SSL/TLS.

- [Instances Windows] Utilisez Active Directory ou AWS Directory Service pour contrôler et surveiller de manière étroite et centralisée l'accès interactif des utilisateurs et des groupes aux instances Windows, et éviter les autorisations des utilisateurs locaux. Évitez également d'utiliser les administrateurs de domaine et créez plutôt des comptes basés sur des rôles plus granulaires et spécifiques à l'application. Just Enough Administration (JEA) permet de gérer les modifications apportées aux instances Windows sans accès interactif ou administrateur. En outre, JEA permet aux entreprises de verrouiller l'accès administratif au sous-ensemble de PowerShell commandes Windows requis pour l'administration des instances. Pour plus d'informations, consultez la section relative à la gestion de l'accès du système d'exploitation à Amazon EC2, dans le livre blanc [AWS Bonnes pratiques de sécurité](#).
- [Instances Windows] Les administrateurs système doivent utiliser des comptes Windows à accès limité pour effectuer leurs activités quotidiennes, et n'augmenter l'accès que lorsque cela est nécessaire pour effectuer des modifications de configuration spécifiques. En outre, n'accédez directement aux instances Windows que lorsque cela est absolument nécessaire. Utilisez plutôt des systèmes de gestion de configuration centralisés tels que EC2 Run Command, Systems Center Configuration Manager (SCCM), Windows PowerShell DSC ou Amazon EC2 Systems Manager (SSM) pour appliquer les modifications aux serveurs Windows.
- Configurez les tables de routage de sous-réseau Amazon VPC avec les routes réseau minimales requises. Par exemple, placez uniquement les instances Amazon EC2 nécessitant un accès direct à Internet dans des sous-réseaux dotés de routes vers une passerelle Internet, et placez uniquement les instances Amazon EC2 nécessitant un accès direct aux réseaux internes dans des sous-réseaux dotés de routes vers une passerelle privée virtuelle.
- Envisagez l'utilisation de groupes de sécurité supplémentaires ou d'interfaces réseau pour contrôler et vérifier le trafic de gestion d'instance Amazon EC2 séparément du trafic d'application régulier. Cette approche permet aux clients de mettre en œuvre des stratégies IAM spéciales pour le contrôle des modifications, ce qui facilite l'audit des modifications apportées aux règles de groupe de sécurité ou aux scripts automatisés de vérification des règles. L'utilisation de plusieurs interfaces réseau fournit également des options supplémentaires pour contrôler le trafic réseau, notamment la possibilité de créer des politiques de routage basées sur l'hôte ou de tirer parti de différentes règles de routage de sous-réseaux VPC en fonction du sous-réseau attribué de l'interface réseau.
- Utilisez AWS Virtual Private Network ou AWS Direct Connect pour établir des connexions privées entre vos réseaux distants et vos VPC. Pour plus d'informations, consultez [Network-to-Amazon VPC Connectivity Options](#).
- Utilisez des [journaux de flux VPC](#) pour surveiller la trafic atteignant vos instances.

- Utilisez [la protection contre les GuardDuty programmes malveillants](#) pour identifier les comportements suspects indiquant la présence de logiciels malveillants sur vos instances susceptibles de compromettre votre charge de travail, de réaffecter des ressources à des fins malveillantes et d'obtenir un accès non autorisé à vos données.
- Utilisez la [surveillance du temps GuardDuty d'exécution](#) pour identifier les menaces potentielles qui pèsent sur vos instances et y répondre. Pour plus d'informations, consultez [Comment fonctionne la surveillance du temps d'exécution avec les instances Amazon EC2](#).
- Utilisez [AWS Security HubReachability Analyzer ou Network Access Analyzer pour vérifier l'absence d'accessibilité involontaire au réseau](#) depuis vos instances.
- Utilisez [EC2 Instance Connect](#) pour vous connecter à vos instances à l'aide de Secure Shell (SSH) sans devoir partager et gérer des clés SSH.
- Utilisez le [gestionnaire de AWS Systems Manager session](#) pour accéder à vos instances à distance au lieu d'ouvrir des ports SSH ou RDP entrants et de gérer des paires de clés.
- Utilisez [AWS Systems Manager Run Command](#) pour automatiser les tâches administratives courantes au lieu de vous connecter à vos instances.
- [Instances Windows] De nombreux rôles du système d'exploitation Windows et des applications professionnelles Microsoft fournissent également des fonctionnalités améliorées, telles que les restrictions de plage d'adresses IP dans IIS, les politiques de filtrage TCP/IP dans Microsoft SQL Server et les politiques de filtre de connexion dans Microsoft Exchange. La fonctionnalité de restriction de réseau au sein de la couche d'application peut fournir des couches supplémentaires de défense pour les serveurs d'applications métier critiques.

Amazon VPC prend en charge des contrôles de sécurité réseau supplémentaires, tels que les passerelles, les serveurs proxy et les options de surveillance du réseau. Pour plus d'informations, consultez la section [Contrôler le trafic réseau](#) dans le guide de l'utilisateur Amazon VPC.

Résilience dans Amazon EC2

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Si vous avez besoin de répliquer vos données ou applications sur des distances géographiques plus importantes, utilisez les Local Zones AWS . Une zone AWS locale est une extension d'une AWS région située à proximité géographique de vos utilisateurs. Les Local Zones ont leurs propres connexions à Internet et prennent en charge AWS Direct Connect. Comme toutes les AWS régions, les Zones AWS Locales sont complètement isolées des autres AWS zones.

Si vous devez répliquer vos données ou applications dans une zone AWS locale, il est AWS recommandé d'utiliser l'une des zones suivantes comme zone de basculement :

- Une autre zone locale
- Une zone de disponibilité dans la région qui n'est pas la zone parent Vous pouvez utiliser la commande [describe-availability-zones](#) pour afficher la zone parent.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section [Infrastructure AWS mondiale](#).

Outre l'infrastructure AWS mondiale, Amazon EC2 propose les fonctionnalités suivantes pour renforcer la résilience de vos données :

- Copie des AMI entre régions
- Copie des instantanés EBS entre régions
- Automatisation des AMI basées sur EBS à l'aide d'Amazon Data Lifecycle Manager
- Automatisation des instantanés EBS à l'aide d'Amazon Data Lifecycle Manager
- Gestion de la santé et de la disponibilité de votre flotte Amazon EC2 Auto Scaling
- Distribution du trafic entrant sur plusieurs instances dans une ou plusieurs zones de disponibilité à l'aide d'Elastic Load Balancing

Validation de la conformité pour Amazon EC2

Pour savoir si un [programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité](#) spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- [Guides de démarrage rapide sur la sécurité et la conformité](#) : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- [Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services](#) : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

 Note

Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le [HIPAA Eligible Services Reference](#).

- AWS Ressources de <https://aws.amazon.com/compliance/resources/> de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- [AWS Guides de conformité destinés aux clients](#) — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- [Évaluation des ressources à l'aide des règles](#) du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- [AWS Security Hub](#)— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez [Référence des contrôles Security Hub](#).
- [Amazon GuardDuty](#) — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider

à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- [AWS Audit Manager](#)— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Identity and Access Management pour Amazon EC2

Vos informations de sécurité vous identifient auprès des services AWS et vous permettent d'utiliser vos AWS ressources de manière illimitée, telles que vos ressources Amazon EC2. Vous pouvez utiliser les fonctions d'Amazon EC2 et AWS Identity and Access Management (IAM) pour permettre aux autres utilisateurs, services et applications d'utiliser vos ressources Amazon EC2 sans partager vos autorisations de sécurité. Vous pouvez utiliser IAM pour contrôler la façon dont les autres utilisateurs utilisent les ressources de votre AWS compte, et vous pouvez utiliser des groupes de sécurité pour contrôler l'accès à vos instances Amazon EC2. Vous pouvez choisir entre une utilisation complète et une utilisation limitée de vos ressources Amazon EC2.

Pour connaître les meilleures pratiques de sécurisation de vos AWS ressources à l'aide d'IAM, consultez [la section Bonnes pratiques de sécurité dans IAM](#).

Table des matières

- [Accès réseau à votre instance](#)
- [Attributs d'autorisation Amazon EC2](#)
- [IAM et Amazon EC2](#)
- [Stratégies IAM pour Amazon EC2](#)
- [AWS politiques gérées pour Amazon EC2](#)
- [Rôles IAM pour Amazon EC2](#)

Accès réseau à votre instance

Un groupe de sécurité fonctionne comme un pare-feu qui contrôle le trafic autorisé à atteindre une ou plusieurs instances. Lorsque vous lancez une instance, vous lui attribuez un ou plusieurs groupes de sécurité. Vous ajoutez des règles à chaque groupe de sécurité qui contrôlent le trafic de l'instance. Vous pouvez modifier les règles d'un groupe de sécurité à tout moment. Les nouvelles règles sont appliquées automatiquement à toutes les instances auxquelles le groupe de sécurité est affecté.

Pour plus d'informations, consultez [Règles des groupes de sécurité](#).

Attributs d'autorisation Amazon EC2

Votre organisation possède peut-être plusieurs AWS comptes. Amazon EC2 vous permet de spécifier des AWS comptes supplémentaires qui peuvent utiliser vos images Amazon Machine Images (AMI) et vos instantanés Amazon EBS. Ces autorisations ne fonctionnent qu'au niveau du AWS compte ; vous ne pouvez pas restreindre les autorisations pour des utilisateurs spécifiques au sein du AWS compte spécifié. Tous les utilisateurs du compte AWS que vous avez spécifiés peuvent utiliser l'AMI ou l'instantané.

Chaque AMI possède un attribut `LaunchPermission` qui contrôle les comptes AWS pouvant accéder à l'AMI. Pour plus d'informations, consultez [Rendre une AMI publique](#).

Chaque instantané Amazon EBS possède un `createVolumePermission` attribut qui contrôle les AWS comptes autorisés à utiliser l'instantané. Pour plus d'informations, consultez [Partager un instantané Amazon EBS](#) dans le guide de l'utilisateur Amazon EBS.

IAM et Amazon EC2

IAM vous permet d'effectuer les tâches suivantes :

- Créez des utilisateurs et des groupes sous votre Compte AWS
- Attribuez des informations de sécurité uniques à chaque utilisateur sous votre Compte AWS
- Contrôlez les autorisations de chaque utilisateur pour effectuer des tâches à l'aide de AWS ressources
- Permettez aux utilisateurs d'un autre utilisateur Compte AWS de partager vos AWS ressources
- Créez des rôles pour vous Compte AWS et définissez les utilisateurs ou les services qui peuvent les assumer
- Utilisez les identités existantes pour que votre entreprise accorde des autorisations pour effectuer des tâches à l'aide de AWS ressources

Grâce à l'utilisation d'IAM avec Amazon EC2, vous pouvez contrôler si les utilisateurs de votre organisation peuvent exécuter une tâche à l'aide d'actions d'API Amazon EC2 particulières et s'ils peuvent utiliser les ressources AWS spécifiques.

Cette rubrique vous aide à répondre aux questions suivantes :

- Comment créer des groupes et des utilisateurs dans IAM ?
- Comment créer une politique ?
- De quelles politiques IAM ai-je besoin pour exécuter des tâches dans Amazon EC2 ?
- Comment accorder des permissions pour exécuter des actions dans Amazon EC2 ?
- Comment attribuer des permissions pour exécuter des actions sur des ressources spécifiques dans Amazon EC2 ?

Création d'utilisateurs, de groupes et de rôles

Vous pouvez créer des utilisateurs et des groupes pour votre compte, Compte AWS puis leur attribuer les autorisations dont ils ont besoin. Il est recommandé aux utilisateurs d'acquérir les autorisations en assumant des rôles IAM.

Un [rôle](#) IAM est une identité IAM que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Un rôle IAM est similaire à un utilisateur IAM dans la mesure où il s'agit d'une AWS identité dotée de politiques d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire. AWS En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. En outre, un rôle ne dispose pas d'informations d'identification standard à long terme comme un mot de passe ou des clés d'accès associées. Au lieu de cela, lorsque vous adoptez un rôle, il vous fournit des informations d'identification de sécurité temporaires pour votre session de rôle. Pour plus d'informations sur la façon de créer des rôles IAM et d'octroyer des autorisations avec ceux-ci, consultez [the section called "Rôles IAM"](#).

Rubriques en relation

Pour plus d'informations sur IAM, consultez les ressources suivantes :

- [Stratégies IAM pour Amazon EC2](#)
- [Rôles IAM pour Amazon EC2](#)
- [AWS Identity and Access Management \(JE SUIS\)](#)
- [Guide de l'utilisateur IAM](#)

Stratégies IAM pour Amazon EC2

Par défaut, les utilisateurs n'ont pas l'autorisation de créer ou de modifier des ressources Amazon EC2, ni d'effectuer des tâches à l'aide de l'API Amazon EC2, de la console Amazon EC2 ou de la CLI. Pour permettre aux utilisateurs de créer ou de modifier des ressources et d'effectuer des tâches, vous devez créer des politiques IAM qui accordent aux utilisateurs l'autorisation d'utiliser les ressources spécifiques et les actions d'API dont ils auront besoin, puis attacher ces politiques aux utilisateurs, aux groupes ou aux rôles IAM qui nécessitent ces autorisations.

Quand vous attachez une stratégie à un utilisateur, à un groupe d'utilisateurs ou à un rôle, celle-ci accorde ou refuse aux utilisateurs l'autorisation d'exécuter les tâches spécifiées sur les ressources spécifiées. Pour des informations plus générales sur les politiques IAM, consultez [Politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la gestion et la création de politiques IAM personnalisées, consultez [Gestion des politiques IAM](#).

Prise en main

Une politique IAM doit accorder ou refuser les autorisations permettant d'utiliser une ou plusieurs actions Amazon EC2. Elle doit aussi spécifier les ressources qui peuvent être utilisées avec l'action : il peut s'agir de toutes les ressources ou, dans certains cas, de ressources spécifiques. La politique peut aussi inclure les conditions que vous appliquez à la ressource.

Amazon EC2 prend partiellement en charge les permissions au niveau des ressources. Cela signifie que pour certaines actions d'API EC2, vous ne pouvez pas spécifier quelle ressource un utilisateur est autorisé à utiliser pour cette action. Au lieu de cela, vous devez autoriser les utilisateurs à utiliser toutes les ressources pour cette action.

Tâche	Sujet
Comprendre la structure de base d'une politique	Syntaxe d'une politique
Définir les actions de votre politique	Actions pour Amazon EC2
Définir les ressources spécifiques de votre politique	Amazon Resource Names (ARN) pour Amazon EC2
Appliquer les conditions à l'utilisation des ressources	Clés de condition pour Amazon EC2

Tâche	Sujet
Utiliser les permissions disponibles au niveau des ressources pour Amazon EC2	Actions, ressources et clés de condition pour Amazon EC2
Tester votre politique	Vérifier que les utilisateurs ont les autorisations requises
Générer une politique IAM	Générer des politiques basées sur l'activité d'accès
Exemple de politiques pour une CLI ou un SDK	Exemples de politiques pour travailler avec le AWS CLI ou un AWS SDK
Exemple de politiques pour la console Amazon EC2	Exemples de politiques à utiliser sur la console Amazon EC2

Octroi d'autorisations aux utilisateurs, aux groupes et aux rôles

Voici des exemples de politiques AWS gérées que vous pouvez utiliser si elles répondent à vos besoins :

- `PowerUserAccess`
- `ReadOnlyAccess`
- `AmazonEC2FullAccess`
- `AmazonEC2ReadOnlyAccess`

Pour plus d'informations, consultez [the section called "AWS politiques gérées"](#).

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :
 - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.
 - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Structure d'une politique

Les rubriques suivantes expliquent la structure d'une politique IAM.

Sommaire

- [Syntaxe d'une politique](#)
- [Actions pour Amazon EC2](#)
- [Autorisations au niveau des ressources prises en charge pour les opérations d'API Amazon EC2](#)
- [Amazon Resource Names \(ARN\) pour Amazon EC2](#)
- [Clés de condition pour Amazon EC2](#)
- [Vérifier que les utilisateurs ont les autorisations requises](#)

Syntaxe d'une politique

Une politique IAM est un document JSON qui se compose d'une ou de plusieurs déclarations. Chaque déclaration est structurée comme suit :

```
{
  "Statement": [{
    "Effect": "effect",
    "Action": "action",
    "Resource": "arn",
    "Condition": {
      "condition": {
        "key": "value"
      }
    }
  ]
}
```

```
}  
]  
}
```

Une déclaration se compose de différents éléments :

- **Effect** : effect peut avoir la valeur `Allow` ou `Deny`. Comme, par défaut, les utilisateurs n'ont pas la permission d'utiliser les ressources et les actions d'API, toutes les demandes sont refusées. Une autorisation explicite remplace l'autorisation par défaut. Un refus explicite remplace toute autorisation.
- **Action** : action désigne l'action d'API spécifique pour laquelle vous accordez ou refusez l'autorisation. Pour en savoir plus sur la spécification d'action, consultez [Actions pour Amazon EC2](#).
- **Resource** : la ressource affectée par l'action. Certaines actions d'API Amazon EC2 vous permettent d'inclure des ressources spécifiques dans votre politique qui peuvent être créées ou modifiées par l'action. Vous spécifiez une ressource à l'aide d'un Amazon Resource Name (ARN) ou du caractère générique (*) pour indiquer que l'instruction s'applique à toutes les ressources. Pour plus d'informations, consultez [Autorisations au niveau des ressources prises en charge pour les opérations d'API Amazon EC2](#).
- **Condition** : les conditions sont facultatives. Elles permettent de contrôler à quel moment votre politique est effective. Pour plus d'informations sur la spécification des conditions pour Amazon EC2, consultez [Clés de condition pour Amazon EC2](#).

Pour plus d'informations sur les exigences de stratégie, consultez [Référence des éléments de stratégie IAM JSON](#) dans le Guide de l'utilisateur IAM. Pour obtenir des déclarations de politique IAM pour Amazon EC2, consultez [Exemples de politiques pour travailler avec le AWS CLI ou un AWS SDK](#).

Actions pour Amazon EC2

Dans une déclaration de politique IAM, vous pouvez spécifier une action d'API à partir de n'importe quel service prenant en charge IAM. Pour Amazon EC2, utilisez le préfixe suivant avec le nom de l'action d'API : `ec2:`. Par exemple : `ec2:RunInstances` et `ec2:CreateImage`.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": ["ec2:action1", "ec2:action2"]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques. Par exemple, vous pouvez spécifier toutes les actions dont le nom commence par le mot « Describe » comme suit :

```
"Action": "ec2:Describe*"
```

Note

Actuellement, les actions d'API Amazon EC2 Describe* ne sont pas compatibles avec les autorisations de niveau ressource. Pour en savoir plus sur les autorisations de ressources pour Amazon EC2, consultez [Stratégies IAM pour Amazon EC2](#).

Pour spécifier toutes les actions d'API Amazon EC2, utilisez le caractère générique * comme suit :

```
"Action": "ec2:*"
```

Pour afficher la liste des actions Amazon EC2, consultez [Actions définies par Amazon EC2](#) dans Référence de l'autorisation de service.

Autorisations au niveau des ressources prises en charge pour les opérations d'API Amazon EC2

Les autorisations au niveau des ressources font référence à la possibilité de spécifier les ressources sur lesquelles les utilisateurs sont autorisés à exécuter des actions. Amazon EC2 prend partiellement en charge les autorisations au niveau des ressources. Cela signifie que pour certaines actions Amazon EC2, vous pouvez contrôler à quel moment les utilisateurs sont autorisés à utiliser ces actions en fonction des conditions qui doivent être satisfaites, ou les ressources spécifiques que les utilisateurs sont autorisés à utiliser. Par exemple, vous pouvez accorder aux utilisateurs les autorisations de lancer des instances, mais uniquement d'un type spécifique et seulement à l'aide d'une AMI spécifique.

Pour spécifier une ressource dans la déclaration de politique IAM, vous utilisez son Amazon Resource Name (ARN). Pour plus d'informations sur la spécification de la valeur de l'ARN, consultez [Amazon Resource Names \(ARN\) pour Amazon EC2](#). Si une action d'API ne prend pas en charge les ARN individuels, utilisez un caractère générique (*) pour spécifier que toutes les ressources peuvent être concernées par l'action.

Pour afficher les tableaux qui identifient les actions d'API Amazon EC2 qui prennent en charge les autorisations au niveau des ressources, ainsi que les ARN et les clés de condition que vous pouvez

utiliser dans une stratégie, consultez la section [Actions, ressources et clés de condition pour Amazon EC2](#).

Notez que vous pouvez appliquer des autorisations au niveau des ressources et basées sur des balises dans les politiques IAM que vous utilisez pour les actions d'API Amazon EC2. Vous bénéficiez ainsi d'un meilleur contrôle sur les ressources qu'un utilisateur peut créer, modifier ou utiliser. Pour plus d'informations, consultez [Accorder l'autorisation de baliser les ressources lors de la création](#).

Amazon Resource Names (ARN) pour Amazon EC2

Chaque déclaration de politique IAM s'applique aux ressources que vous spécifiez à l'aide de leur ARN.

Un ARN obéit à la syntaxe générale suivante :

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

web

Le service (par exemple, ec2).

region

La région de la ressource (par exemple, us-east-1).

id-compte

L'identifiant du AWS compte, sans tiret (par exemple,123456789012).

resourceType

Le type de ressource (par exemple, instance).

chemin de la ressource

Un chemin qui identifie la ressource. Vous pouvez utiliser le caractère générique * dans vos chemins.

Par exemple, vous pouvez indiquer une instance spécifique (i-1234567890abcdef0) dans votre déclaration à l'aide de son ARN comme suit :

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Vous pouvez spécifier toutes les instances qui appartiennent à un compte spécifique à l'aide du caractère générique * comme suit :

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Vous pouvez aussi spécifier toutes les ressources Amazon EC2 qui appartiennent à un compte spécifique à l'aide du caractère générique * comme suit :

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Pour spécifier toutes les ressources, ou si une action d'API spécifique ne prend pas en charge les ARN, utilisez le caractère générique * dans l'élément Resource comme suit :

```
"Resource": "*"
```

De nombreuses actions d'API Amazon EC2 nécessitent plusieurs ressources. Par exemple, comme `AttachVolume` attache un volume Amazon EBS à une instance, un utilisateur doit avoir les autorisations nécessaires pour utiliser le volume et l'instance. Pour spécifier plusieurs ressources dans une seule déclaration, séparez leurs ARN par des virgules, comme suit :

```
"Resource": ["arn1", "arn2"]
```

Pour obtenir la liste des ARN pour les ressources Amazon EC2, consultez la section [Types de ressources définis par Amazon EC2](#).

Clés de condition pour Amazon EC2

Dans une déclaration de politique, vous pouvez, le cas échéant, spécifier des conditions qui contrôlent à quel moment la déclaration est effective. Chaque condition contient une ou plusieurs paires clé-valeur. Les clés de condition ne sont pas sensibles à la casse. Nous avons défini des clés de condition AWS globales, ainsi que des clés de condition supplémentaires spécifiques au service.

Pour obtenir la liste des clés de condition spécifiques au service pour Amazon EC2, consultez la section [Clés de condition pour Amazon EC2](#). Amazon EC2 implémente également les clés de condition AWS globales. Pour plus d'informations, consultez [Informations disponibles dans toutes les demandes](#) dans le Guide de l'utilisateur IAM.

Pour utiliser une clé de condition dans votre stratégie IAM, utilisez l'instruction `Condition`. Par exemple, la politique suivante accorde aux utilisateurs l'autorisation d'ajouter et de supprimer des

règles entrantes et sortantes pour n'importe quel groupe de sécurité. Elle utilise la clé de condition `ec2:Vpc` pour spécifier que ces actions ne peuvent être effectuées que sur des groupes de sécurité dans un VPC spécifique.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress"],
    "Resource": "arn:aws:ec2:region:account:security-group/*",
    "Condition": {
      "StringEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
      }
    }
  ]
}
```

Si vous spécifiez plusieurs conditions ou plusieurs clés dans une même condition, elles sont analysées à l'aide d'une opération logique AND. Si vous spécifiez une seule condition avec plusieurs valeurs pour une clé, la condition est analysée à l'aide d'une opération logique OR. Pour que les autorisations soient accordées, toutes les conditions doivent être satisfaites.

Vous pouvez aussi utiliser des espaces réservés quand vous spécifiez des conditions. Pour plus d'informations, consultez [Éléments des politiques IAM : variables et balises](#) dans le Guide de l'utilisateur IAM.

Important

Plusieurs clés de condition sont propres à une ressource et certaines actions d'API utilisent plusieurs ressources. Si vous écrivez une stratégie avec une clé de condition, utilisez l'élément `Resource` de la déclaration pour spécifier la ressource à laquelle la clé de condition s'applique. Dans le cas contraire, la politique peut empêcher totalement les utilisateurs d'exécuter l'action, car le contrôle de la condition échoue pour les ressources auxquelles la clé de condition ne s'applique pas. Si vous ne voulez pas spécifier de ressource ou si vous avez écrit l'élément `Action` de votre stratégie pour inclure plusieurs actions d'API,

vous devez utiliser le type de condition `...IfExists` pour garantir que la clé de condition est ignorée pour les ressources qui ne l'utilisent pas. Pour plus d'informations, voir... [IfExists Conditions énoncées](#) dans le guide de l'utilisateur IAM.

Toutes les actions Amazon EC2 prennent en charge les clés de condition `aws:RequestedRegion` et `ec2:Region`. Pour plus d'informations, consultez [Exemple : Restreindre l'accès à une région spécifique](#).

Clé de condition `ec2:SourceInstanceARN`

La clé de condition `ec2:SourceInstanceARN` peut être utilisée pour les conditions qui spécifient le nom ARN de l'instance à partir de laquelle une demande a été effectuée. Il s'agit d'une clé de condition AWS globale qui n'est pas spécifique à un service. Pour examiner des exemples de politique, consultez [Amazon EC2 : autoriser une instance EC2 à attacher et détacher des volumes](#) et [Exemple : autoriser une instance spécifique à afficher les ressources d'autres AWS services](#). La clé `ec2:SourceInstanceARN` ne peut pas être utilisée comme variable pour renseigner le nom ARN de l'élément `Resource` dans une instruction.

Pour obtenir des déclarations de politique pour Amazon EC2, consultez [Exemples de politiques pour travailler avec le AWS CLI ou un AWS SDK](#).

Clé de condition `ec2:Attribute`

La clé de condition `ec2:Attribute` peut être utilisée pour les conditions qui filtrent l'accès par un attribut d'une ressource. La clé de condition ne prend en charge que les propriétés de type de données primitif (telles qu'une chaîne ou un entier) ou les [AttributeValue](#) objets complexes dotés uniquement d'une propriété `Value` (comme la description ou les `ImdsSupport` objets de l'action API [ModifyImageAttribute](#)).

Important

La clé de condition ne peut pas être utilisée avec des objets complexes dotés de plusieurs propriétés, tels que l'`LaunchPermission` objet de l'action API [ModifyImageAttribute](#).

Par exemple, la politique suivante utilise la clé de `ec2:Attribute/Description` condition pour filtrer l'accès en fonction de l'objet `Description` complexe de l'action API `ModifyImageAttribute`. La clé

de condition n'autorise que les demandes qui modifient la description d'une image pour `Production` ou `Development`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

L'exemple de politique suivant utilise la clé de `ec2:Attribute` condition pour filtrer l'accès en fonction de la propriété primitive `Attribute` de l'action API `ModifyImageAttribute`. La clé de condition refuse toutes les demandes qui tentent de modifier la description d'une image.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
}
```

Clés de condition **ec2:ResourceID**

Lorsque vous utilisez les clés de condition `ec2:ResourceID` suivantes avec les actions d'API spécifiées, la valeur de la clé de condition est utilisée pour spécifier la ressource résultante créée par l'action d'API. Les clés de condition `ec2:ResourceID` ne peuvent pas être utilisées pour spécifier une ressource source spécifiée dans la demande d'API. Si vous utilisez l'une des clés de condition `ec2:ResourceID` suivantes avec une API spécifiée, vous devez alors toujours spécifier le caractère générique (*). Si vous spécifiez une valeur différente, la condition se résout toujours en * pendant l'exécution. Par exemple, pour utiliser la clé de `ec2:ImageId` condition avec l'`CopyImageAPI`, vous devez spécifier la clé de condition comme suit :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Clé de condition	Action d'API			
<code>ec2:DhcpOptionsID</code>	<ul style="list-style-type: none"> CreateDhcpOptions 			
<code>ec2:ImageID</code>	<ul style="list-style-type: none"> CopyImage CreateImage 			

Clé de condition	Action d'API			
	<ul style="list-style-type: none"> ImportImage RegisterImage 			
ec2:InstanceID	<ul style="list-style-type: none"> RunInstances ImportInstance 			
ec2:InternetGatewayID	<ul style="list-style-type: none"> CreateInternetPasserelle 			
ec2:NetworkACLID	<ul style="list-style-type: none"> CreateNetworkAcl 			
ec2:NetworkInterfaceID	<ul style="list-style-type: none"> CreateNetworkInterface 			
ec2:PlacementGroupName	<ul style="list-style-type: none"> CreatePlacementGroupe 			
ec2:RouteTableID	<ul style="list-style-type: none"> CreateRouteTableau 			

Clé de condition	Action d'API			
ec2:SecurityGroupID	<ul style="list-style-type: none">CreateSecurityGroup			
ec2:SnapshotID	<ul style="list-style-type: none">CopySnapshotCreateSnapshotCreateSnapshotsImportSnapshots			
ec2:SubnetID	<ul style="list-style-type: none">CreateSubnet			
ec2:VolumeID	<ul style="list-style-type: none">CreateVolumeImportVolume			
ec2:VpcID	<ul style="list-style-type: none">CreateVpc			

Clé de condition	Action d'API			
ec2:VpcPeeringConnectionID	<ul style="list-style-type: none">CreateVpcPeeringConnection			

Nous vous recommandons d'éviter d'utiliser les clés de condition `ec2:ResourceID` avec ces actions d'API. Si vous devez filtrer l'accès en fonction d'ID de ressources spécifiques, nous vous recommandons plutôt de le faire à l'aide de l'élément de politique `Resource`, comme suit :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1:image/ami-01234567890abcdef"
    }
  ]
}
```

Vérifier que les utilisateurs ont les autorisations requises

Après que vous avez créé une politique IAM, il vous est recommandé de vérifier si elle accorde aux utilisateurs les autorisations d'utiliser les actions d'API et ressources particulières dont ils ont besoin avant que vous ne placiez la politique en production.

D'abord, créez un utilisateur à des fins de test, puis attachez la politique IAM que vous avez créée à l'utilisateur test. Ensuite, créez une demande en tant qu'utilisateur test.

Si l'action Amazon EC2 que vous testez crée ou modifie une ressource, vous devez effectuer la demande à l'aide du paramètre `DryRun` (ou exécuter la commande AWS CLI avec l'option `--dry-run`). Dans ce cas, l'appel conclut le contrôle d'autorisation, mais non l'opération. Par exemple, vous pouvez vérifier si l'utilisateur peut terminer une instance particulière sans réellement l'achever. Si l'utilisateur a les autorisations requises, la demande retourne `DryRunOperation` ; sinon, elle retourne `UnauthorizedOperation`.

Si la politique n'accorde pas à l'utilisateur les autorisations que vous escomptiez, ou si elles sont trop excessives, vous pouvez ajuster la politique selon vos besoins et la tester à nouveau jusqu'à ce que vous obteniez les résultats souhaités.

Important

La propagation des modifications de la politique peut durer plusieurs minutes avant qu'elles ne prennent effet. Par conséquent, il est recommandé que vous laissiez s'écouler cinq minutes avant de tester les mises à jour de votre politique.

Si un contrôle d'autorisation échoue, la demande retourne un message codé avec les informations de diagnostic. Vous pouvez décoder le message à l'aide de l'action `DecodeAuthorizationMessage`. Pour plus d'informations, consultez [DecodeAuthorizationMessage](#) dans la référence de l'AWS Security Token Service API et [decode-authorization-message](#) dans la référence des commandes AWS CLI.

Accorder l'autorisation de baliser les ressources lors de la création

Certaines actions d'API Amazon EC2 de création de ressources vous permettent de spécifier des balises lorsque vous créez la ressource. Vous pouvez utiliser des balises de ressource pour implémenter le contrôle basé sur les attributs (ABAC). Pour plus d'informations, consultez [Etiqueter vos ressources](#) et [Contrôler l'accès aux ressources EC2 à l'aide des balises de ressources](#).

Pour permettre aux utilisateurs d'attribuer des balises aux ressources au moment de la création, ils doivent avoir les autorisations d'utiliser l'action qui crée la ressource (par exemple, `ec2:RunInstances` ou `ec2:CreateVolume`). Si les balises sont spécifiées dans l'action de création de ressources, Amazon effectue une autorisation supplémentaire sur l'action `ec2:CreateTags` pour vérifier si les utilisateurs sont autorisés à créer des balises. Par conséquent, les utilisateurs doivent également avoir des autorisations explicites d'utiliser l'action `ec2:CreateTags`.

Dans la définition de stratégie IAM de l'action `ec2:CreateTags`, utilisez l'élément `Condition` avec la clé de condition `ec2:CreateAction` pour accorder des autorisations de balisage à l'action qui crée la ressource.

L'exemple suivant illustre une politique qui permet aux utilisateurs de lancer des instances et d'appliquer des balises aux instances et aux volumes pendant le lancement. Les utilisateurs ne sont

pas autorisés à attribuer des balises aux ressources existantes (ils ne peuvent pas appeler l'action `ec2:CreateTags` directement).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

De même, la politique suivante permet aux utilisateurs de créer des volumes et appliquer des balises à des volumes pendant la création de volume. Les utilisateurs ne sont pas autorisés à attribuer des balises aux ressources existantes (ils ne peuvent pas appeler l'action `ec2:CreateTags` directement).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVolume"
      ],
      "Resource": "*"
    },
    {
```

```
"Effect": "Allow",
"Action": [
  "ec2:CreateTags"
],
"Resource": "arn:aws:ec2:region:account:*/*",
"Condition": {
  "StringEquals": {
    "ec2:CreateAction" : "CreateVolume"
  }
}
]
```

L'action `ec2:CreateTags` est uniquement évaluée si les balises sont appliquées pendant l'action de création de ressources. Par conséquent, un utilisateur qui est autorisé à créer une ressource (en supposant qu'il n'existe aucune condition de balisage) n'a pas besoin des autorisations d'utiliser l'action `ec2:CreateTags` si aucune balise n'est spécifié dans la demande. Toutefois, si l'utilisateur essaie de créer une ressource avec des balises, la demande échoue s'il n'a pas les autorisations d'utiliser l'action `ec2:CreateTags`.

L'action `ec2:CreateTags` est également évaluée si des balises sont fournies dans un modèle de lancement. Pour un exemple de politique, consultez [Balises dans un modèle de lancement](#).

Contrôler l'accès à des balises spécifiques

Vous pouvez utiliser des conditions supplémentaires dans l'élément `Condition` de vos stratégies IAM pour contrôler les clés de balise et les valeurs qui peuvent être appliquées aux ressources.

Les clés de condition suivantes peuvent être utilisées avec les exemples de la section précédente :

- `aws:RequestTag` : Pour indiquer qu'une clé de balise ou une clé et valeur de balise particulière doit être présente dans une demande. D'autres balises peuvent également être spécifiées dans la demande.
- Utilisez avec l'opérateur de condition `StringEquals` pour appliquer une combinaison de clé de balise et de valeur spécifique ; par exemple, pour appliquer la balise `cost-center=cc123` :

```
"StringEquals": { "aws:RequestTag/cost-center": "cc123" }
```

- A utiliser avec l'opération de condition `StringLike` pour appliquer une clé de balise spécifique dans la demande ; par exemple, pour appliquer la clé de balise `purpose` :

```
"StringLike": { "aws:RequestTag/purpose": "*" }
```

- `aws:TagKeys` : Pour appliquer les clés de balise qui sont utilisées dans la demande.
- A utiliser avec le modificateur `ForAllValues` pour appliquer des clés de balise spécifiques si celles-ci sont fournies dans la demande (si les balises sont spécifiées dans la demande, seules les clés de balise spécifiques sont autorisées ; aucune autre balise n'est autorisée). Par exemple, les clés de balise `environment` ou `cost-center` sont autorisées :

```
"ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
```

- A utiliser avec le modificateur `ForAnyValue` pour appliquer la présence d'au moins l'une des clés de balise spécifiées dans la demande. Par exemple, au moins l'une des clés de balise `environment` ou `webserver` doit être présente dans la demande :

```
"ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
```

Ces clés de condition peuvent être appliqués aux actions de création de ressources qui prennent en charge le balisage ainsi qu'aux actions `ec2:CreateTags` et `ec2:DeleteTags`. Pour savoir si une action d'API Amazon EC2 prend en charge le balisage, consultez la section [Actions, ressources et clés de condition pour Amazon EC2](#).

Pour forcer les utilisateurs à spécifier des balises quand ils créent une ressource, vous devez utiliser la clé de condition `aws:RequestTag` ou la clé de condition `aws:TagKeys` avec le modificateur `ForAnyValue` sur l'action de création de ressources. L'action `ec2:CreateTags` n'est pas évaluée si un utilisateur ne spécifie pas de balises pour l'action de création de ressources.

Pour les conditions, la clé de condition n'est pas sensible à la casse et la valeur de la condition est sensible à la casse. Par conséquent pour forcer la sensibilité à la casse d'une clé de balise, utilisez la clé de condition `aws:TagKeys`, où la clé de balise est indiquée comme une valeur dans la condition.

Par exemple les stratégies IAM, consultez [Exemples de politiques pour travailler avec le AWS CLI ou un AWS SDK](#). Pour plus d'informations sur les conditions à valeur multiples, consultez [Création d'une condition qui teste plusieurs valeurs de clés](#) dans le IAM Guide de l'utilisateur.

Contrôler l'accès aux ressources EC2 à l'aide des balises de ressources

Lorsque vous créez une politique IAM qui accorde aux utilisateurs l'autorisation d'utiliser les ressources EC2, vous pouvez inclure des informations de balise dans l'élément `Condition` de

la politique pour contrôler l'accès en fonction des balises. Ceci est connu sous le nom de contrôle d'accès basé sur les attributs (ABAC). ABAC vous offre un meilleur contrôle sur les ressources qu'un utilisateur peut modifier, utiliser ou supprimer. Pour plus d'informations, consultez [Présentation d'ABAC pour AWS](#).

Par exemple, vous pouvez créer une stratégie qui permet aux utilisateurs de résilier une instance, mais qui refuse l'action si l'instance possède la balise `environment=production`. Pour ce faire, vous utilisez la clé de condition `aws:ResourceTag` pour autoriser ou refuser l'accès à la ressource en fonction des balises attachées à la ressource.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Pour savoir si une action d'API Amazon EC2 prend en charge le contrôle d'accès à l'aide de la clé de condition `aws:ResourceTag`, consultez la section [Actions, ressources et clés de condition pour Amazon EC2](#). Notez que les actions `Describe` ne prennent pas en charge les autorisations au niveau des ressources, vous devez donc les spécifier dans une instruction distincte sans condition.

Par exemple les stratégies IAM, consultez [Exemples de politiques pour travailler avec le AWS CLI ou un AWS SDK](#).

Si vous autorisez ou refusez à des utilisateurs l'accès à des ressources en fonction de balises, vous devez envisager de refuser de manière explicite la possibilité pour les utilisateurs d'ajouter ces balises ou de les supprimer des mêmes ressources. Sinon, il sera possible pour un utilisateur de contourner vos restrictions et d'obtenir l'accès à une ressource en modifiant ses balises.

Exemples de politiques pour travailler avec le AWS CLI ou un AWS SDK

Vous devez accorder aux utilisateurs les autorisations dont ils ont besoin pour Amazon EC2 à l'aide des politiques IAM. Les exemples suivants illustrent des instructions de politique que vous pouvez utiliser pour contrôler les autorisations des utilisateurs sur Amazon EC2. Ces politiques sont conçues pour les demandes effectuées avec le AWS CLI ou un AWS SDK. Pour plus d'informations, consultez [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM. Pour obtenir des exemples de stratégies à utiliser sur la console Amazon EC2, consultez [Exemples de politiques à utiliser sur la console Amazon EC2](#). Pour obtenir des exemples de stratégies IAM spécifiques à Amazon VPC, consultez [Identity and Access Management pour Amazon VPC](#).

Dans les exemples suivants, remplacez chaque *user input placeholder* (espace réservé pour l'entrée utilisateur) avec vos propres informations.

Exemples

- [Exemple : accès en lecture seule](#)
- [Exemple : Restreindre l'accès à une région spécifique](#)
- [Utiliser des instances](#)
- [Instances de lancement \(RunInstances\)](#)
- [Utiliser instances Spot](#)
- [Exemple : Utiliser instances réservées](#)
- [Exemple : Baliser des ressources](#)
- [Exemple : Utiliser des rôles IAM](#)
- [Exemple : Utiliser des tables de routage](#)
- [Exemple : autoriser une instance spécifique à afficher les ressources d'autres AWS services](#)
- [Exemple : Utiliser des modèles de lancement](#)
- [Utiliser des métadonnées d'instance](#)
- [Travaillez avec les volumes et les instantanés Amazon EBS](#)

Exemple : accès en lecture seule

La stratégie suivante accorde aux utilisateurs les autorisations d'utiliser toutes les actions d'API Amazon EC2 dont les noms commencent par `Describe`. L'élément `Resource` utilise un caractère générique pour indiquer que les utilisateurs peuvent spécifier toutes les ressources avec ces actions d'API. Le caractère générique `*` est également nécessaire dans les cas où l'action d'API ne prend pas en charge les autorisations au niveau des ressources. Pour en savoir plus sur les ARN que vous pouvez utiliser avec les actions d'API Amazon EC2, consultez la section [Actions, ressources et clés de condition pour Amazon EC2](#).

Les utilisateurs n'ont pas l'autorisation d'effectuer la moindre action sur les ressources (à moins qu'une autre déclaration ne leur accorde l'autorisation de le faire), car, par défaut, l'autorisation d'utiliser les actions d'API leur est refusée.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
  ]
}
```

```
]
}
```

Exemple : Restreindre l'accès à une région spécifique

La politique suivante refuse aux utilisateurs l'autorisation d'utiliser toutes les actions d'API Amazon EC2 à moins que la région soit Europe (Francfort). Elle utilise la clé de condition globale `aws:RequestedRegion` qui est prise en charge par toutes les actions d'API Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
}
```

Sinon, vous pouvez utiliser la clé de condition `ec2:Region`, qui est spécifique à Amazon EC2 et qui est prise en charge par toutes les actions d'API Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

```
}
```

Utiliser des instances

Exemples

- [Exemple : Décrire, lancer, arrêter, démarrer et résilier toutes les instances](#)
- [Exemple : Décrire toutes les instances, et arrêter, démarrer et résilier uniquement des instances particulières](#)

Exemple : Décrire, lancer, arrêter, démarrer et résilier toutes les instances

La stratégie suivante autorise les utilisateurs à effectuer les actions d'API spécifiées dans l'élément `Action`. L'élément `Resource` utilise un caractère générique `*` pour indiquer que les utilisateurs peuvent spécifier toutes les ressources avec ces actions d'API. Le caractère générique `*` est également nécessaire dans les cas où l'action d'API ne prend pas en charge les autorisations au niveau des ressources. Pour en savoir plus sur les ARN que vous pouvez utiliser avec les actions d'API Amazon EC2, consultez la section [Actions, ressources et clés de condition pour Amazon EC2](#).

Les utilisateurs n'ont pas l'autorisation d'utiliser d'autres actions d'API (à moins qu'une autre déclaration ne leur accorde l'autorisation de le faire), car, par défaut, l'autorisation d'utiliser les actions d'API leur est refusée.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

```
]
}
```

Exemple : Décrire toutes les instances, et arrêter, démarrer et résilier uniquement des instances particulières

La stratégie suivante autorise les utilisateurs à décrire toutes les instances, à démarrer et à arrêter uniquement les instances i-1234567890abcdef0 et i-0598c7d356eba48d7, et à ne terminer que les instances de la région Région USA Est (Virginie du N.) (us-east-1) avec la balise de ressource "purpose=test".

La première déclaration utilise un caractère générique * pour l'élément Resource de façon à indiquer que les utilisateurs peuvent spécifier toutes les ressources avec l'action ; dans le cas présent, ils peuvent afficher toutes les instances. Le caractère générique * est également nécessaire dans les cas où l'action d'API ne prend pas en charge les autorisations au niveau des ressources (dans le cas présent, ec2:DescribeInstances). Pour en savoir plus sur les ARN que vous pouvez utiliser avec les actions d'API Amazon EC2, consultez la section [Actions, ressources et clés de condition pour Amazon EC2](#).

La deuxième déclaration utilise des permissions au niveau des ressources pour les actions StopInstances et StartInstances. Les instances spécifiques sont indiquées par leurs ARN dans l'élément Resource.

La troisième déclaration permet aux utilisateurs de résilier toutes les instances de la région USA Est (Virginie du Nordus-east-1) () qui appartiennent au AWS compte spécifié, mais uniquement lorsque l'instance possède le tag "purpose=test". L'élément Condition stipule quand la déclaration de stratégie est en vigueur.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ]
    }
  ]
}
```

```
    ],
    "Resource": [
      "arn:aws:ec2:us-east-1:account-id:instance/i-1234567890abcdef0",
      "arn:aws:ec2:us-east-1:account-id:instance/i-0598c7d356eba48d7"
    ]
  },
  {
    "Effect": "Allow",
    "Action": "ec2:TerminateInstances",
    "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/purpose": "test"
      }
    }
  }
]
```

Instances de lancement (RunInstances)

L'action d'[RunInstances](#) API lance une ou plusieurs instances à la demande ou une ou plusieurs instances ponctuelles. RunInstances nécessite une AMI et crée une instance. Les utilisateurs peuvent spécifier une paire de clés et un groupe de sécurité dans la demande. Le lancement dans un VPC nécessite un sous-réseau et crée une interface réseau. Le lancement à partir d'une AMI basée sur des volumes Amazon EBS crée un volume. Par conséquent, l'utilisateur doit être autorisé à utiliser ces ressources Amazon EC2. Vous pouvez créer une déclaration de stratégie qui requiert que les utilisateurs spécifient un paramètre facultatif sur RunInstances, ou limitent les utilisateurs à certaines valeurs pour tel ou tel paramètre.

Pour en savoir plus sur les autorisations au niveau des ressources requises pour lancer une instance, consultez la section [Actions, ressources et clés de condition pour Amazon EC2](#).

Par défaut, les utilisateurs ne sont pas autorisés à décrire, démarrer, arrêter ni résilier les instances obtenues. Une solution pour accorder aux utilisateurs l'autorisation de gérer les instances obtenues consiste à créer une balise spécifique pour chaque instance, puis à créer une déclaration qui leur permet de gérer les instances avec cette balise. Pour plus d'informations, consultez [Utiliser des instances](#).

Ressources

- [AMI](#)
- [Types d'instance](#)
- [Sous-réseaux](#)
- [Volumes EBS](#)
- [Balises](#)
- [Balises dans un modèle de lancement](#)
- [GPU Elastic](#)
- [Modèles de lancement](#)

AMI

La stratégie suivante permet aux utilisateurs de lancer les instances en n'utilisant que les AMI spécifiés, `ami-9e1670f7` et `ami-45cf5c3c`. Les utilisateurs ne peuvent pas lancer une instance à l'aide d'autres AMI (à moins qu'une autre déclaration n'accorde aux utilisateurs l'autorisation de le faire) ni sur un sous-réseau.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-9e1670f7",
        "arn:aws:ec2:region::image/ami-45cf5c3c",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:network-interface/*"
      ]
    }
  ]
}
```

À titre d'autre solution, la politique suivante permet aux utilisateurs de lancer les instances à partir de toutes les AMI appartenant à Amazon, ou à certains partenaires de confiance et vérifiés. L'élément

Condition de la première déclaration+ teste si `ec2:Owner` est `amazon`. Les utilisateurs ne peuvent pas lancer une instance à l'aide d'autres AMI (à moins qu'une autre déclaration n'accorde aux utilisateurs l'autorisation de le faire) ni sur un sous-réseau.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:Owner": "amazon"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group*"
      ]
    }
  ]
}
```

Types d'instance

La stratégie suivante permet aux utilisateurs de lancer des instances uniquement à l'aide du type d'instance `t2.micro` ou `t2.small`, ce que vous pourriez faire pour contrôler les coûts. Les utilisateurs ne peuvent pas lancer d'instances plus grandes parce que l'élément `Condition` de la première déclaration teste si `ec2:InstanceType` est `t2.micro` ou `t2.small`.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region:account-id:instance/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:InstanceType": ["t2.micro", "t2.small"]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account-id:subnet/*",
      "arn:aws:ec2:region:account-id:network-interface/*",
      "arn:aws:ec2:region:account-id:volume/*",
      "arn:aws:ec2:region:account-id:key-pair/*",
      "arn:aws:ec2:region:account-id:security-group*"
    ]
  }
]
}

```

Vous pouvez également créer une stratégie qui refuse aux utilisateurs l'autorisation de lancer des instances, à l'exception des types d'instance `t2.micro` et `t2.small`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {

```

```

        "ec2:InstanceType": ["t2.micro", "t2.small"]
    }
}
},
{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*"
    ]
}
]
}

```

Sous-réseaux

La stratégie suivante permet aux utilisateurs de lancer les instances en n'utilisant que le sous-réseau spécifié, subnet-**12345678**. Le groupe ne peut pas lancer d'instance sur un autre sous-réseau (à moins qu'une autre déclaration n'accorde aux utilisateurs l'autorisation de le faire).

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region:account-id:subnet/subnet-12345678",
                "arn:aws:ec2:region:account-id:network-interface/*",
                "arn:aws:ec2:region:account-id:instance/*",
                "arn:aws:ec2:region:account-id:volume/*",
                "arn:aws:ec2:region::image/ami-*",
                "arn:aws:ec2:region:account-id:key-pair/*",
                "arn:aws:ec2:region:account-id:security-group/*"
            ]
        }
    ]
}

```

```
}
```

Vous pouvez également créer une politique qui refuse aux utilisateurs l'autorisation de lancer une instance sur un autre sous-réseau. La déclaration agit ainsi en refusant l'autorisation de créer une interface réseau, à l'exception de l'emplacement où le sous-réseau subnet-**12345678** est spécifié. Ce refus se substitue à toute autre politique créée pour autoriser le lancement d'instances sur d'autres sous-réseaux.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region:account-id:network-interface/*"
      ],
      "Condition": {
        "ArnNotEquals": {
          "ec2:Subnet": "arn:aws:ec2:region:account-id:subnet/subnet-12345678"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*"
      ]
    }
  ]
}
```

Volumes EBS

La politique suivante permet aux utilisateurs de lancer des instances uniquement si les volumes EBS pour l'instance sont chiffrés. L'utilisateur doit lancer une instance à partir d'une AMI qui a été créée avec des instantanés chiffrés afin de garantir le chiffrement du volume racine. N'importe quel volume supplémentaire que l'utilisateur attache à l'instance pendant le lancement doit aussi être chiffré.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Bool": {
          "ec2:Encrypted": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:image/ami-*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group*"
      ]
    }
  ]
}
```

Balises

Baliser les instances lors de la création

La politique suivante permet aux utilisateurs de lancer des instances et d'attribuer des balises aux instances lors de la création. Pour les actions de création de ressources qui appliquent des balises,

les utilisateurs doivent être autorisés à effectuer l'action `CreateTags`. La deuxième déclaration utilise la clé de condition `ec2:CreateAction` pour permettre aux utilisateurs de créer des balises uniquement dans le cadre de `RunInstances` et uniquement pour des instances. Les utilisateurs ne peuvent pas attribuer de balises aux ressources existantes, et ils ne peuvent pas attribuer de balises aux volumes à l'aide de la demande `RunInstances`.

Pour plus d'informations, consultez [Accorder l'autorisation de baliser les ressources lors de la création](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Baliser des instances et des volumes lors de la création avec des balises spécifiques

La stratégie suivante inclut la clé de condition `aws:RequestTag` qui exige aux utilisateurs d'attribuer des balises aux instances et aux volumes créés par `RunInstances` avec les balises `environment=production` et `purpose=webserver`. Si les utilisateurs ne transmettent pas ces balises spécifiques ou s'ils ne spécifient pas du tout de balises, la demande échoue.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "ec2:RunInstances"
    ],
    "Resource": [
      "arn:aws:ec2:region::image/*",
      "arn:aws:ec2:region:account-id:subnet/*",
      "arn:aws:ec2:region:account-id:network-interface/*",
      "arn:aws:ec2:region:account-id:security-group/*",
      "arn:aws:ec2:region:account-id:key-pair/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:RunInstances"
    ],
    "Resource": [
      "arn:aws:ec2:region:account-id:volume/*",
      "arn:aws:ec2:region:account-id:instance/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/environment": "production" ,
        "aws:RequestTag/purpose": "webserver"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:region:account-id:*/*",
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction" : "RunInstances"
      }
    }
  }
]
```

```
}
```

Baliser des instances et des volumes lors de la création avec au moins une balise spécifique

La stratégie suivante utilise le modificateur `ForAnyValue` sur la condition `aws:TagKeys` pour indiquer qu'au moins une balise doit être spécifiée dans la demande, et elle doit comporter la clé `environment` ou `webserver`. La balise doit être appliquée à la fois aux instances et aux volumes. Toutes les valeurs de balise peuvent être spécifiées dans la demande.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:region:image/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:security-group/*",
        "arn:aws:ec2:region:account-id:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": ["environment", "webserver"]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
```

```

        "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:region:account-id:*/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
        }
    }
}
]
}

```

Si les instances sont balisées lors de la création, elles doivent être balisées avec une balise spécifique

Dans la stratégie suivante, les utilisateurs ne doivent pas spécifier les balises dans la demande, mais s'ils le font, la balise doit être `purpose=test`. Aucune autre balise n'est autorisée. Les utilisateurs peuvent appliquer des balises à n'importe quelle ressource pouvant être balisée dans la demande `RunInstances`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/purpose": "test",
          "ec2:CreateAction" : "RunInstances"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": "purpose"
        }
      }
    }
  ]
}

```

```

    }
  }
}
]
}

```

Pour interdire à toute personne appelée tag sur Create for RunInstances

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRun",
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1::image/*",
        "arn:aws:ec2:us-east-1:*:subnet/*",
        "arn:aws:ec2:us-east-1:*:network-interface/*",
        "arn:aws:ec2:us-east-1:*:security-group/*",
        "arn:aws:ec2:us-east-1:*:key-pair/*",
        "arn:aws:ec2:us-east-1:*:volume/*",
        "arn:aws:ec2:us-east-1:*:instance/*",
        "arn:aws:ec2:us-east-1:*:spot-instances-request*"
      ]
    },
    {
      "Sid": "VisualEditor0",
      "Effect": "Deny",
      "Action": "ec2:CreateTags",
      "Resource": "*"
    }
  ]
}

```

N'autoriser que des balises spécifiques pour spot-instances-request. Incohérence surprise numéro 2 entre en jeu ici. Dans des circonstances normales, si vous ne spécifiez aucune balise, vous n'êtes pas authentifié. Dans ce cas spot-instances-request, cette politique ne sera pas évaluée s'il n'y a

pas de spot-instances-request balises, de sorte qu'une demande Spot on Run sans étiquette sera acceptée.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRun",
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:image/*",
        "arn:aws:ec2:us-east-1:*:subnet/*",
        "arn:aws:ec2:us-east-1:*:network-interface/*",
        "arn:aws:ec2:us-east-1:*:security-group/*",
        "arn:aws:ec2:us-east-1:*:key-pair/*",
        "arn:aws:ec2:us-east-1:*:volume/*",
        "arn:aws:ec2:us-east-1:*:instance/*",
      ]
    },
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "production"
        }
      }
    }
  ]
}
```

Balises dans un modèle de lancement

Dans l'exemple suivant, les utilisateurs peuvent lancer des instances, mais uniquement s'ils utilisent un modèle de lancement spécifique (lt-09477bcd97b0d310e). La clé de condition `ec2:IsLaunchTemplateResource` empêche les utilisateurs de remplacer les ressources spécifiées dans le modèle de lancement. La seconde partie de la déclaration permet aux utilisateurs

de baliser les instances à la création. Cette partie de la déclaration est nécessaire si des balises sont spécifiées pour l'instance dans le modèle de lancement.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d310e"
        },
        "Bool": {
          "ec2:IsLaunchTemplateResource": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

GPU Elastic

Dans la politique suivante, les utilisateurs peuvent lancer une instance et spécifier un GPU Elastic à attacher à l'instance. Les utilisateurs peuvent lancer des instances dans n'importe quelle région, mais ils peuvent uniquement attacher un GPU Elastic lors d'un lancement dans la région `us-east-2`.

La clé de condition `ec2:ElasticGpuType` garantit que les instances utilisent le type de GPU élastique `eg1.medium` ou `eg1.large`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:*:account-id:elastic-gpu/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:Region": "us-east-2",
          "ec2:ElasticGpuType": [
            "eg1.medium",
            "eg1.large"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2::*:image/ami-*",
        "arn:aws:ec2:*:account-id:network-interface/*",
        "arn:aws:ec2:*:account-id:instance/*",
        "arn:aws:ec2:*:account-id:subnet/*",
        "arn:aws:ec2:*:account-id:volume/*",
        "arn:aws:ec2:*:account-id:key-pair/*",
        "arn:aws:ec2:*:account-id:security-group*"
      ]
    }
  ]
}
```

Modèles de lancement

Dans l'exemple suivant, les utilisateurs peuvent lancer des instances, mais uniquement s'ils utilisent un modèle de lancement spécifique (lt-09477bcd97b0d310e). Les utilisateurs peuvent remplacer des paramètres dans le modèle de lancement en spécifiant dans l'action RunInstances.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
        }
      }
    }
  ]
}
```

Dans cet exemple, les utilisateurs peuvent lancer des instances uniquement s'ils utilisent un modèle de lancement. La stratégie utilise la clé de condition `ec2:IsLaunchTemplateResource` pour empêcher les utilisateurs de remplacer les ARN préexistants dans le modèle de lancement.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
        },
        "Bool": {
          "ec2:IsLaunchTemplateResource": "true"
        }
      }
    }
  ]
}
```

Dans l'exemple suivant, une politique permet aux utilisateurs de lancer des instances, mais uniquement s'ils utilisent un modèle de lancement. Les utilisateurs ne peuvent pas remplacer

les paramètres du sous-réseau et de l'interface réseau dans la demande ; ceux-ci ne peuvent être spécifiés que dans le modèle de lancement. La première partie de l'instruction utilise l'[NotResource](#) élément pour autoriser toutes les autres ressources à l'exception des sous-réseaux et des interfaces réseau. La seconde partie de la déclaration autorise les ressources des sous-réseaux et des interfaces réseau, mais uniquement si elles proviennent du modèle de lancement.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:region:account-id:subnet/*",
                    "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:region:account-id:subnet/*",
                  "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
        },
        "Bool": {
          "ec2:IsLaunchTemplateResource": "true"
        }
      }
    }
  ]
}
```

Dans l'exemple suivant, les utilisateurs sont autorisés à lancer des instances uniquement s'ils utilisent un modèle de lancement et seulement si celui-ci contient la balise Purpose=Webservers. Les utilisateurs ne peuvent pas remplacer les paramètres de modèle de lancement dans l'action RunInstances.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
        "ArnLike": {
          "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
        },
        "Bool": {
          "ec2:IsLaunchTemplateResource": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Webservers"
        }
      }
    }
  ]
}
```

Utiliser instances Spot

Vous pouvez utiliser cette RunInstances action pour créer des demandes d'instance Spot et étiqueter les demandes d'instance Spot lors de la création. La ressource à spécifier RunInstances est `spot-instances-request`.

La ressource `spot-instances-request` est évaluée dans la stratégie IAM comme suit :

- Si vous ne balisez pas une demande d'instance Spot lors de la création, Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la RunInstances déclaration.
- Si vous balisez une demande d'instance Spot lors de la création, Amazon EC2 évalue la `spot-instances-request` ressource dans le relevé. RunInstances

Par conséquent, pour la ressource `spot-instances-request`, les règles suivantes s'appliquent à la stratégie IAM :

- Si vous avez l'habitude de créer une demande d'instance ponctuelle et que vous n'avez pas l'intention de baliser la demande d'instance ponctuelle lors de la création, vous n'avez pas besoin d'autoriser explicitement la `spot-instances-request` ressource ; l'appel aboutira.
- Si vous avez l'habitude de créer une demande d'instance Spot et que vous avez l'intention de baliser la demande d'instance Spot lors de sa création, vous devez inclure la `spot-instances-request` ressource RunInstances dans l'instruction d'autorisation, sinon l'appel échouera.
- Si vous avez l'habitude de créer une demande d'instance Spot et que vous avez l'intention de baliser la demande d'instance Spot lors de sa création, vous devez spécifier la `spot-instances-request` ressource ou le `*` caractère générique dans `CreateTags` l'instruction d'autorisation, sinon l'appel échouera.

Vous pouvez demander des instances Spot en utilisant `RunInstances` ou `RequestSpotInstances`. Les exemples de politiques IAM suivants s'appliquent uniquement lorsque vous demandez des instances Spot à l'aide `RunInstances` de.

Exemple : demandez des instances ponctuelles en utilisant `RunInstances`

La politique suivante permet aux utilisateurs de demander des instances Spot en utilisant l'`RunInstances` action. La `spot-instances-request` ressource, créée par `RunInstances`, demande des instances Spot.

Note

À utiliser `RunInstances` pour créer des demandes d'instance Spot, vous pouvez omettre `spot-instances-request` de la Resource liste si vous n'avez pas l'intention de baliser les demandes d'instance Spot lors de la création. Cela est dû au fait qu'Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la `RunInstances` déclaration si la demande d'instance Spot n'est pas balisée lors de la création.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "AllowRun",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances"
    ],
    "Resource": [
        "arn:aws:ec2:us-east-1:image/*",
        "arn:aws:ec2:us-east-1:*:subnet/*",
        "arn:aws:ec2:us-east-1:*:network-interface/*",
        "arn:aws:ec2:us-east-1:*:security-group/*",
        "arn:aws:ec2:us-east-1:*:key-pair/*",
        "arn:aws:ec2:us-east-1:*:volume/*",
        "arn:aws:ec2:us-east-1:*:instance/*",
        "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
    ]
}
]
}

```

Warning

NON PRIS EN CHARGE — Exemple : refuser aux utilisateurs l'autorisation de demander des instances Spot en utilisant RunInstances

La stratégie suivante n'est pas prise en charge pour la ressource `spot-instances-request`.

La politique suivante vise à donner aux utilisateurs l'autorisation de lancer instances à la demande, mais à refuser aux utilisateurs l'autorisation de demander instances Spot. La `spot-instances-request` ressource, créée par RunInstances, est la ressource qui demande les instances Spot. La deuxième déclaration vise à refuser l' RunInstances action pour la `spot-instances-request` ressource. Toutefois, cette condition n'est pas prise en charge car Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la RunInstances déclaration si la demande d'instance Spot n'est pas balisée lors de la création.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRun",
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"

```

```
    ],
    "Resource": [
        "arn:aws:ec2:us-east-1::image/*",
        "arn:aws:ec2:us-east-1::*:subnet/*",
        "arn:aws:ec2:us-east-1::*:network-interface/*",
        "arn:aws:ec2:us-east-1::*:security-group/*",
        "arn:aws:ec2:us-east-1::*:key-pair/*",
        "arn:aws:ec2:us-east-1::*:volume/*",
        "arn:aws:ec2:us-east-1::*:instance/*"
    ]
},
{
    "Sid": "DenySpotInstancesRequests - NOT SUPPORTED - DO NOT USE!",
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:us-east-1::*:spot-instances-request/*"
}
]
```

Exemple : étiquetez les demandes d'instance Spot lors de la création

La politique suivante permet aux utilisateurs de baliser toutes les ressources créées lors du lancement de l'instance. La première instruction permet RunInstances de créer les ressources listées. La `spot-instances-request` ressource, créée par RunInstances, est la ressource qui demande les instances Spot. La deuxième instruction fournit un caractère générique `*` pour permettre à toutes les ressources d'être balisées lorsqu'elles sont créées au lancement de l'instance.

Note

Si vous balisez une demande d'instance Spot lors de la création, Amazon EC2 évalue la `spot-instances-request` ressource dans le relevé. RunInstances Par conséquent, vous devez autoriser explicitement la `spot-instances-request` ressource pour l' RunInstances action, sinon l'appel échouera.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
{
  "Sid": "AllowRun",
  "Effect": "Allow",
  "Action": [
    "ec2:RunInstances"
  ],
  "Resource": [
    "arn:aws:ec2:us-east-1:image/*",
    "arn:aws:ec2:us-east-1:*:subnet/*",
    "arn:aws:ec2:us-east-1:*:network-interface/*",
    "arn:aws:ec2:us-east-1:*:security-group/*",
    "arn:aws:ec2:us-east-1:*:key-pair/*",
    "arn:aws:ec2:us-east-1:*:volume/*",
    "arn:aws:ec2:us-east-1:*:instance/*",
    "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
  ]
},
{
  "Sid": "TagResources",
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": "*"
}
]
```

Exemple : refuser l'étiquette lors de la création des demandes d'instance Spot

La politique suivante refuse aux utilisateurs l'autorisation de baliser les ressources créées lors du lancement de l'instance.

La première instruction permet RunInstances de créer les ressources listées. La `spot-instances-request` ressource, créée par RunInstances, est la ressource qui demande les instances Spot. La deuxième instruction fournit un caractère générique `*` pour refuser toutes les ressources en cours de balisage lorsqu'elles sont créées au lancement de l'instance. Si `spot-instances-request` ou toute autre ressource est étiquetée lors de la création, l' RunInstances appel échouera.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRun",
      "Effect": "Allow",
```

```

    "Action": [
      "ec2:RunInstances"
    ],
    "Resource": [
      "arn:aws:ec2:us-east-1::image/*",
      "arn:aws:ec2:us-east-1:*:subnet/*",
      "arn:aws:ec2:us-east-1:*:network-interface/*",
      "arn:aws:ec2:us-east-1:*:security-group/*",
      "arn:aws:ec2:us-east-1:*:key-pair/*",
      "arn:aws:ec2:us-east-1:*:volume/*",
      "arn:aws:ec2:us-east-1:*:instance/*",
      "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
    ]
  },
  {
    "Sid": "DenyTagResources",
    "Effect": "Deny",
    "Action": "ec2:CreateTags",
    "Resource": "*"
  }
]
}

```

Warning

NON PRIS EN CHARGE, exemple : autoriser la création d'une demande d'instance Spot uniquement si une étiquette spécifique lui est attribuée

La stratégie suivante n'est pas prise en charge pour la ressource `spot-instances-request`.

La politique suivante vise à accorder RunInstances l'autorisation de créer une demande d'instance Spot uniquement si la demande est étiquetée avec une balise spécifique.

La première instruction permet RunInstances de créer les ressources listées.

La deuxième instruction est destinée à accorder aux utilisateurs l'autorisation de créer une demande d'instance Spot uniquement si la demande a l'étiquette `environment=production`. Si cette condition est appliquée à d'autres ressources créées par RunInstances, le fait de ne pas spécifier de balises entraîne une `Unauthenticated` erreur. Toutefois, si aucune balise n'est spécifiée pour la demande d'instance Spot, Amazon EC2 n'évalue pas la `spot-instances-request` ressource dans la RunInstances déclaration, ce qui entraîne la création de demandes d'instance Spot non étiquetées par RunInstances

Notez que la spécification d'une autre balise `environment=production` entraîne une `Unauthenticated` erreur, car si un utilisateur balise une demande d'instance Spot, Amazon EC2 évalue la `spot-instances-request` ressource dans la déclaration. `RunInstances`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRun",
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1::image/*",
        "arn:aws:ec2:us-east-1:*:subnet/*",
        "arn:aws:ec2:us-east-1:*:network-interface/*",
        "arn:aws:ec2:us-east-1:*:security-group/*",
        "arn:aws:ec2:us-east-1:*:key-pair/*",
        "arn:aws:ec2:us-east-1:*:volume/*",
        "arn:aws:ec2:us-east-1:*:instance/*"
      ]
    },
    {
      "Sid": "RequestSpotInstancesOnlyIfTagIs_environment=production - NOT
SUPPORTED - DO NOT USE!",
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "production"
        }
      }
    },
    {
      "Sid": "TagResources",
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "*"
    }
  ]
}
```

```
}
```

Exemple : refuser la création d'une demande d'instance Spot si une étiquette spécifique lui est attribuée

La politique suivante refuse RunInstances l'autorisation de créer une demande d'instance Spot si la demande est étiquetée avec `environment=production`.

La première instruction permet RunInstances de créer les ressources listées.

La deuxième instruction refuse aux utilisateurs l'autorisation de créer une demande d'instance Spot si la demande a l'étiquette `environment=production`. La spécification `environment=production` en tant que balise entraîne une erreur `Unauthenticated`. La spécification d'autres étiquettes ou l'absence d'étiquettes entraînera la création d'une demande d'instance Spot.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRun",
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1::image/*",
        "arn:aws:ec2:us-east-1:*:subnet/*",
        "arn:aws:ec2:us-east-1:*:network-interface/*",
        "arn:aws:ec2:us-east-1:*:security-group/*",
        "arn:aws:ec2:us-east-1:*:key-pair/*",
        "arn:aws:ec2:us-east-1:*:volume/*",
        "arn:aws:ec2:us-east-1:*:instance/*",
        "arn:aws:ec2:us-east-1:*:spot-instances-request*"
      ]
    },
    {
      "Sid": "DenySpotInstancesRequests",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
```

```
    "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/environment": "production"
      }
    }
  },
  {
    "Sid": "TagResources",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "*"
  }
]
```

Exemple : Utiliser instances réservées

La politique suivante autorise les utilisateurs à afficher, modifier et acheter les instances réservées de votre compte.

Il n'est pas possible de définir des autorisations au niveau des ressources pour les instances réservées individuelles. Cette politique signifie que les utilisateurs ont accès à toutes les instances réservées du compte.

L'élément `Resource` utilise un caractère générique `*` pour indiquer que les utilisateurs peuvent spécifier toutes les ressources avec l'action. Dans ce cas, ils peuvent afficher et modifier toutes les Instances réservées du compte. Ils peuvent aussi acheter des instances réservées à l'aide des informations d'identification du compte. Le caractère générique `*` est également nécessaire dans les cas où l'action d'API ne prend pas en charge les autorisations au niveau des ressources.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ]
    }
  ]
}
```

```
    ],
    "Resource": "*"
  }
]
```

Pour permettre aux utilisateurs d'afficher et de modifier les instances réservées de votre compte, mais pas d'acheter de nouvelles instances réservées.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemple : Baliser des ressources

La stratégie suivante permet aux utilisateurs d'utiliser l'action `CreateTags` pour appliquer des balises à une instance uniquement si la balise contient la clé `environment` et la valeur `production`. Aucune autre identification n'est autorisée et l'utilisateur ne peut pas étiqueter d'autres types de ressources.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:instance/*",
      "Condition": {
```

```

        "StringEquals": {
            "aws:RequestTag/environment": "production"
        }
    }
}
]
}

```

La politique suivante permet aux utilisateurs d'attribuer des balises à n'importe quelle ressource pouvant être balisée qui possède déjà une balise avec une clé de `owner` et une valeur du nom d'utilisateur. En outre, les utilisateurs doivent spécifier une balise avec une clé de `anycompany:environment-type` et une valeur `test` ou `prod` dans la demande. Les utilisateurs peuvent spécifier des balises supplémentaires dans la demande.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/anycompany:environment-type": ["test", "prod"],
          "aws:ResourceTag/owner": "${aws:username}"
        }
      }
    }
  ]
}

```

Vous pouvez créer une politique IAM qui permet aux utilisateurs de supprimer des balises spécifiques pour une ressource. Par exemple, la stratégie suivante permet aux utilisateurs de supprimer les balises pour un volume si les clés de balise spécifiées dans la demande sont `environment` ou `cost-center`. N'importe quelle valeur peut être spécifiée pour la balise, mais la clé de balise doit correspondre à l'une des clés spécifiées.

Note

Si vous supprimez une ressource, toutes les balises associées à celle-ci sont également supprimées. Les utilisateurs n'ont pas besoin d'être autorisés à effectuer l'action `ec2:DeleteTags` pour supprimer une ressource comportant des balises ; ils doivent seulement être autorisés à effectuer l'action de suppression.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment", "cost-center"]
        }
      }
    }
  ]
}
```

Cette politique permet aux utilisateurs de supprimer uniquement la balise `environment=prod` sur n'importe quelle ressource et uniquement si la ressource porte déjà une balise avec une clé de `owner` et une valeur du nom d'utilisateur. Les utilisateurs ne peuvent pas supprimer d'autres balises pour une ressource.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",

```

```

    "aws:ResourceTag/owner": "${aws:username}"
  },
  "ForAllValues:StringEquals": {
    "aws:TagKeys": ["environment"]
  }
}
]
}

```

Exemple : Utiliser des rôles IAM

La stratégie suivante permet aux utilisateurs d'attacher, de remplacer et de détacher un rôle IAM pour les instances ayant la balise `department=test`. Le remplacement ou le détachement d'un rôle IAM nécessite un ID d'association. Par conséquent, la stratégie accorde également aux utilisateurs l'autorisation d'utiliser l'action `ec2:DescribeIamInstanceProfileAssociations`.

Les utilisateurs doivent être autorisés à utiliser l'action `iam:PassRole` pour transmettre le rôle à l'instance.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    }
  ]
}

```

```
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::account-id:role/DevTeam*"
}
]
}
```

La politique suivante permet aux utilisateurs d'attacher, de remplacer et de détacher un rôle IAM pour une instance. Les utilisateurs ne peuvent attacher ou remplacer que des rôles IAM dont les noms commencent par `TestRole-`. Pour l'action `iam:PassRole`, veillez à indiquer le nom du rôle IAM et non celui du profil d'instance (si ces noms ne sont pas identiques). Pour plus d'informations, consultez [Profils d'instance](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/TestRole-*"
    }
  ]
}
```

Exemple : Utiliser des tables de routage

La stratégie suivante permet aux utilisateurs d'ajouter, de supprimer et de remplacer des routes pour les tables de routage associées au VPC `vpc-ec43eb89` uniquement. Pour spécifier un VPC pour la clé de condition `ec2:Vpc`, vous devez spécifier l'ARN complet du VPC.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteRoute",
        "ec2:CreateRoute",
        "ec2:ReplaceRoute"
      ],
      "Resource": [
        "arn:aws:ec2:region:account-id:route-table/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-ec43eb89"
        }
      }
    }
  ]
}
```

Exemple : autoriser une instance spécifique à afficher les ressources d'autres AWS services

Voici un exemple de politique que vous pouvez attacher à un rôle IAM. La politique permet à une instance de visualiser les ressources de différents AWS services. Elle utilise la clé de condition `ec2:SourceInstanceARN` pour spécifier que l'instance dont émane la demande doit être l'instance `i-093452212644b0dd6`. Si le même rôle IAM est associé à une autre instance, l'autre instance ne peut effectuer aucune de ces actions.

La `ec2:SourceInstanceARN` clé est une clé de condition AWS globale, elle peut donc être utilisée pour d'autres actions de service, et pas uniquement pour Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "dynamodb:ListTables",
```

```

        "rds:DescribeDBInstances"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "ArnEquals": {
            "ec2:SourceInstanceARN": "arn:aws:ec2:region:account-id:instance/
i-093452212644b0dd6"
        }
    }
}

```

Exemple : Utiliser des modèles de lancement

La stratégie suivante permet aux utilisateurs de créer une version du modèle de lancement et de modifier un modèle de lancement, mais uniquement pour un modèle spécifique (lt-*09477bcd97b0d3abc*). Les utilisateurs ne peuvent pas utiliser d'autres modèles de lancement.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d3abc"
    }
  ]
}

```

La stratégie suivante permet aux utilisateurs de supprimer un modèle de lancement et une version du modèle de lancement, sous réserve que le modèle de lancement contienne la balise Purpose=Testing.

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```
{
  "Action": [
    "ec2:DeleteLaunchTemplate",
    "ec2:DeleteLaunchTemplateVersions"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/Purpose": "Testing"
    }
  }
}
```

Utiliser des métadonnées d'instance

Les stratégies suivantes garantissent que les utilisateurs peuvent uniquement récupérer les [métadonnées d'instance](#) à l'aide d'Service des métadonnées d'instance Version 2 (IMDSv2). Vous pouvez combiner les quatre politiques suivantes en une seule politique avec quatre instructions. Une fois combinée, vous pouvez l'utiliser en tant que politique de contrôle de service (SCP). Elle peut fonctionner aussi bien qu'une stratégie de refus que vous appliquez à une stratégie IAM existante (en retirant et en limitant les autorisations existantes), ou qu'une stratégie de contrôle de service appliquée globalement sur un compte, une unité organisationnelle ou l'ensemble d'une organisation.

Note

Les politiques d'options de RunInstances métadonnées suivantes doivent être utilisées conjointement avec une politique qui donne les autorisations principales pour lancer une instance RunInstances. Si le principal ne dispose pas également d' RunInstances autorisations, il ne sera pas en mesure de lancer une instance. Pour plus d'informations, consultez les stratégies dans [Utiliser des instances](#) et [Instances de lancement \(RunInstances\)](#).

Important

Si vous utilisez des groupes Auto Scaling et que vous devez exiger l'utilisation d'IMDSv2 sur toutes les nouvelles instances, vos groupes Auto Scaling doivent utiliser des modèles de lancement.

Lorsqu'un groupe Auto Scaling utilise un modèle de lancement, les autorisations `ec2:RunInstances` du principal IAM sont vérifiées lors de la création d'un nouveau groupe Auto Scaling. Elles sont également vérifiées lorsqu'un groupe Auto Scaling existant est mis à jour pour utiliser un nouveau modèle de lancement ou une nouvelle version d'un modèle de lancement.

Les restrictions relatives à l'utilisation d'IMDSv1 sur les principaux IAM pour `RunInstances` sont uniquement vérifiées lorsqu'un groupe Auto Scaling utilisant un modèle de lancement est créé ou mis à jour. Pour un groupe Auto Scaling configuré pour utiliser le modèle de lancement `Latest` ou `Default`, les autorisations ne sont pas vérifiées lors de la création d'une nouvelle version du modèle de lancement. Pour que les autorisations soient vérifiées, vous devez configurer le groupe Auto Scaling pour qu'il utilise une version spécifique du modèle de lancement.

Pour appliquer l'utilisation d'IMDSv2 sur des instances lancées par des groupes Auto Scaling, les étapes supplémentaires suivantes sont requises :

1. Désactivez l'utilisation des configurations de lancement pour tous les comptes de votre organisation à l'aide des politiques de contrôle de service (SCP) ou des limites d'autorisations IAM pour les nouvelles entités créées. Pour les principaux IAM existants disposant d'autorisations de groupe Auto Scaling, mettez à jour leurs politiques associées avec cette clé de condition. Pour désactiver l'utilisation des configurations de lancement, créez ou modifiez la stratégie SCP, les limites d'autorisations ou la stratégie IAM avec la clé de condition `"autoscaling:LaunchConfigurationName"` avec la valeur spécifiée comme `null`.
2. Pour les nouveaux modèles de lancement, configurez les options de métadonnées d'instance dans le modèle de lancement. Pour les modèles de lancement existants, créez une nouvelle version du modèle de lancement et configurez les options de métadonnées d'instance dans la nouvelle version.
3. Dans la politique donnant à tout principal l'autorisation d'utiliser un modèle de lancement, restreignez l'association de `$latest` et de `$default` en spécifiant `"autoscaling:LaunchTemplateVersionSpecified": "true"`. En restreignant l'utilisation à une version spécifique d'un modèle de lancement, vous pouvez vous assurer

que les nouvelles instances seront lancées à l'aide de la version dans laquelle les options de métadonnées d'instance sont configurées. Pour plus d'informations, consultez la section [LaunchTemplateSpécification](#) dans le manuel Amazon EC2 Auto Scaling API Reference, en particulier le `Version` paramètre.

4. Pour un groupe Auto Scaling qui utilise une configuration de lancement, remplacez la configuration de lancement par un modèle de lancement. Pour plus d'informations, voir [Remplacement d'une configuration de lancement par un modèle de lancement](#) dans le Amazon EC2 Auto Scaling Guide de l'utilisateur.
5. Pour un groupe Auto Scaling qui utilise un modèle de lancement, assurez-vous qu'il utilise un nouveau modèle de lancement avec les options de métadonnées d'instance configurées ou qu'il utilise une nouvelle version du modèle de lancement actuel avec les options de métadonnées d'instance configurées. Pour plus d'informations, consultez [update-auto-scaling-group](#) le manuel de référence des AWS CLI commandes.

Exemples

- [Exigence d'utilisation d'IMDSv2](#)
- [Refus de la désactivation d'IMDSv2](#)
- [Spécification d'une durée de vie \(hop limit\) maximale](#)
- [Restriction des personnes habilitées à modifier les options de métadonnées d'instance](#)
- [Exigence de récupération des informations d'identification de rôle à partir d'IMDSv2](#)

Exigence d'utilisation d'IMDSv2

La politique suivante indique que vous ne pouvez pas appeler l' `RunInstances` API à moins que l'instance ne soit également activée pour exiger l'utilisation d'IMDSv2 (indiqué par `"ec2:MetadataHttpTokens": "required"`). Si vous ne spécifiez pas que l'instance nécessite IMDSv2, une `UnauthorizedOperation` erreur s'affiche lorsque vous appelez l' `RunInstances` API.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireImdsV2",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
```

```

    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  }
]
}

```

Refus de la désactivation d'IMDSv2

La politique suivante indique que vous ne pouvez pas appeler l'API `ModifyInstanceMetadataOptions` et autoriser l'option `IMDSv1` ou `IMDSv2`. Si vous appelez l'API `ModifyInstanceMetadataOptions`, l'attribut `HttpTokens` doit être défini sur `required`.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyIMDSv1HttpTokensModification",
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:Attribute/HttpTokens": "required"
      },
      "Null": {
        "ec2:Attribute/HttpTokens": false
      }
    }
  }]
}

```

Spécification d'une durée de vie (hop limit) maximale

La politique suivante indique que vous ne pouvez pas appeler l' `RunInstances` API sauf si vous spécifiez également une limite de sauts, et la limite de sauts ne peut pas être supérieure à 3. Si vous ne le faites pas, une `UnauthorizedOperation` erreur s'affiche lorsque vous appelez l' `RunInstances` API.

```

{

```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "MaxImdsHopLimit",
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  }
]
}

```

Restriction des personnes habilitées à modifier les options de métadonnées d'instance

La politique suivante permet uniquement aux utilisateurs ayant le rôle `ec2-imds-admins` d'apporter des modifications aux options de métadonnées de l'instance. Si un principal autre que le `ec2-imds-admins` rôle essaie d'appeler l' `ModifyInstanceMetadataOptions` API, il recevra une `UnauthorizedOperation` erreur. Cette instruction peut être utilisée pour contrôler l'utilisation de l' `ModifyInstanceMetadataOptions` API ; il n'existe actuellement aucun contrôle d'accès précis (conditions) pour l' `ModifyInstanceMetadataOptions` API.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyImdsAdminsToModifySettings",
      "Effect": "Deny",
      "Action": "ec2:ModifyInstanceMetadataOptions",
      "Resource": "*",
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": "arn:aws:iam:*:*:role/ec2-imds-admins"
        }
      }
    }
  ]
}

```

Exigence de récupération des informations d'identification de rôle à partir d'IMDSv2

La politique suivante indique que si cette politique est appliquée à un rôle endossé par le service EC2, et que les informations d'identification obtenues sont utilisées pour signer une demande, la demande doit alors être signée par les informations d'identification de rôle EC2 extraites d'IMDSv2. Sinon, tous ses appels d'API recevront l'erreur `UnauthorizedOperation`. Cette instruction/politique peut être appliquée de manière générale car, si la demande n'est pas signée par les informations d'identification de rôle EC2, elle n'a aucun effet.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireAllEc2RolesToUseV2",
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "NumericLessThan": {
          "ec2:RoleDelivery": "2.0"
        }
      }
    }
  ]
}
```

Travaillez avec les volumes et les instantanés Amazon EBS

Pour des exemples de politiques relatives à l'utilisation des volumes et des instantanés Amazon EBS, consultez la section [Exemples de politiques basées sur l'identité pour Amazon EBS](#).

Exemples de politiques à utiliser sur la console Amazon EC2

Vous devez accorder aux utilisateurs les autorisations dont ils ont besoin pour Amazon EC2 à l'aide des politiques IAM. Vous pouvez utiliser les politiques IAM pour accorder aux utilisateurs les autorisations d'afficher et d'utiliser des ressources spécifiques sur la console Amazon EC2. Vous pouvez utiliser les exemples de politiques présentés dans la section précédente ; toutefois, ils sont conçus pour les demandes effectuées avec le AWS CLI ou un AWS SDK. Pour plus d'informations, veuillez consulter [Exemples de politiques pour travailler avec le AWS CLI ou un AWS SDK](#) et la rubrique [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM.

Puisque la console utilise des actions d'API supplémentaires pour ses fonctions, ces politiques peuvent ne pas fonctionner comme escompté. Par exemple, un utilisateur n'ayant que l'autorisation d'utiliser l'action d'API `DescribeVolumes` rencontre une erreur s'il tente d'afficher les volumes sur la console. Cette section illustre les politiques qui permettent aux utilisateurs d'utiliser des parties spécifiques de la console. Pour plus d'informations sur la création de politiques pour la console Amazon EC2, consultez le billet de blog sur la AWS sécurité suivant : [Octroyer aux utilisateurs l'autorisation de travailler dans la console Amazon EC2](#).

Tip

Pour vous aider à découvrir les actions d'API requises pour exécuter des tâches sur la console, vous pouvez utiliser un service tel que AWS CloudTrail. Pour plus d'informations, veuillez consulter le [Guide de l'utilisateur AWS CloudTrail](#). Si votre politique n'accorde pas l'autorisation de créer ou de modifier une ressource spécifique, la console affiche un message codé avec les informations de diagnostic. Vous pouvez décoder le message à l'aide de l'action [DecodeAuthorizationMessage](#) API ou de la AWS STS commande [decode-authorization-message](#) dans le. AWS CLI

Exemples

- [Exemple : accès en lecture seule](#)
- [Exemple : utiliser l'assistant de lancement d'instances d'EC2](#)
- [Exemple : Utiliser des groupes de sécurité](#)
- [Exemple : Utiliser des adresses IP Elastic](#)
- [Exemple : Utiliser instances réservées](#)

Exemple : accès en lecture seule

Pour permettre aux utilisateurs d'afficher toutes les ressources sur la console Amazon EC2, vous pouvez utiliser la même stratégie que l'exemple suivant : [Exemple : accès en lecture seule](#). Les utilisateurs ne peuvent pas exécuter d'actions sur ces ressources ou créer des ressources, à moins qu'une autre déclaration ne leur accorde l'autorisation de le faire.

Afficher les instances, les AMI et les instantanés

Vous pouvez aussi fournir un accès en lecture seule à un sous-ensemble de ressources. Pour ce faire, remplacez le caractère générique * de l'action d'API `ec2:Describe` par les actions

ec2:Describe spécifiques de chaque ressource. La politique suivante permet aux utilisateurs d'afficher l'ensemble des instances, AMI et instantanés sur la console Amazon EC2. L'action ec2:DescribeTags permet aux utilisateurs d'afficher les AMI publiques. La console nécessite les informations de balisage pour afficher les AMI publiques. Néanmoins, vous pouvez supprimer cette action pour permettre aux utilisateurs de voir uniquement les AMI privées.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeTags",
      "ec2:DescribeSnapshots"
    ],
    "Resource": "*"
  }
]
```

Note

Comme les actions d'API Amazon EC2 ec2:Describe* ne prennent pas en charge les autorisations au niveau des ressources, vous ne pouvez pas contrôler les ressources individuelles que les utilisateurs peuvent afficher sur la console. Par conséquent, le caractère générique * est nécessaire dans l'élément Resource de la déclaration ci-dessus. Pour en savoir plus sur les ARN que vous pouvez utiliser avec les actions d'API Amazon EC2, consultez la section [Actions, ressources et clés de condition pour Amazon EC2](#).

Afficher les instances et CloudWatch les métriques

La politique suivante permet aux utilisateurs de consulter les instances dans la console Amazon EC2, ainsi que les CloudWatch alarmes et les métriques dans l'onglet Surveillance de la page Instances. La console Amazon EC2 utilise l' CloudWatch API pour afficher les alarmes et les métriques. Vous devez donc autoriser les utilisateurs à utiliser les actions cloudwatch:DescribeAlarms,cloudwatch:DescribeAlarmsForMetric,

```
cloudwatch:ListMetricscloudwatch:GetMetricStatistics,  
etccloudwatch:GetMetricData.
```

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": [  
      "ec2:DescribeInstances",  
      "ec2:DescribeInstanceTypes",  
      "cloudwatch:DescribeAlarms",  
      "cloudwatch:DescribeAlarmsForMetric",  
      "cloudwatch:ListMetrics",  
      "cloudwatch:GetMetricStatistics",  
      "cloudwatch:GetMetricData"  
    ],  
    "Resource": "*"   
  }  
]
```

Exemple : utiliser l'assistant de lancement d'instances d'EC2

L'assistant de lancement d'instances d'Amazon EC2 se compose d'un écran contenant les options de configuration et de lancement d'une instance. Votre politique doit inclure l'autorisation d'utiliser les actions d'API qui permettent aux utilisateurs d'utiliser les options de l'Assistant. Si votre politique n'inclut pas l'autorisation d'utiliser ces actions, certains éléments de l'Assistant ne peuvent pas se charger correctement et les utilisateurs ne peuvent pas exécuter de lancement.

Accès de base à l'assistant de lancement d'instances

Pour exécuter un lancement avec succès, les utilisateurs doivent avoir l'autorisation d'utiliser l'action d'API `ec2:RunInstances`, ainsi qu'au moins les actions d'API suivantes :

- `ec2:DescribeImages` : afficher et sélectionner une AMI.
- `ec2:DescribeInstanceTypes` : afficher et sélectionner un type d'instance.
- `ec2:DescribeVpcs` : afficher les options réseau disponibles.
- `ec2:DescribeSubnets` : afficher tous les sous-réseaux disponibles pour le VPC choisi.
- `ec2:DescribeSecurityGroups` ou `ec2:CreateSecurityGroup` : pour afficher et sélectionner un groupe de sécurité existant, ou en créer un nouveau.

- `ec2:DescribeKeyPairs` ou `ec2:CreateKeyPair` : pour sélectionner une paire de clés existante ou en créer une nouvelle.
- `ec2:AuthorizeSecurityGroupIngress` : ajouter des règles entrantes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*"
    }
  ]
}
```

Vous pouvez ajouter des actions d'API à votre politique pour fournir plus d'options pour les utilisateurs, par exemple :

- `ec2:DescribeAvailabilityZones` : afficher et sélectionner une zone de disponibilité spécifique.
- `ec2:DescribeNetworkInterfaces` : afficher et sélectionner les interfaces réseau existantes pour le sous-réseau sélectionné.
- Pour ajouter des règles sortantes à des groupes de sécurité VPC, les utilisateurs doivent recevoir l'autorisation d'utiliser l'action d'API `ec2:AuthorizeSecurityGroupEgress`. Pour modifier

ou supprimer des règles existantes, les utilisateurs doivent recevoir l'autorisation d'utiliser l'action d'API `ec2:RevokeSecurityGroup*` appropriée.

- `ec2:CreateTags` : Pour attribuer des balises aux ressources qui sont créées par `RunInstances`. Pour plus d'informations, consultez [Accorder l'autorisation de baliser les ressources lors de la création](#). Si les utilisateurs n'ont pas l'autorisation d'utiliser cette action et qu'ils essaient d'appliquer des balises sur la page de balisage de l'assistant de lancement d'instances, le lancement échoue.

Important

La spécification d'un Name (Nom) lors du lancement d'une instance crée une balise et nécessite l'action `ec2:CreateTags`. Veillez à accorder aux utilisateurs l'autorisation d'utiliser l'action `ec2:CreateTags`, car cela limite votre capacité à utiliser la clé de condition `aws:ResourceTag` pour restreindre leur utilisation d'autres ressources. Si vous accordez aux utilisateurs l'autorisation d'utiliser l'action `ec2:CreateTags`, ils peuvent modifier la balise d'une ressource afin de contourner ces restrictions. Pour plus d'informations, consultez [Contrôler l'accès aux ressources EC2 à l'aide des balises de ressources](#).

- Pour utiliser des paramètres Systems Manager lors de la sélection d'une AMI, vous devez ajouter `ssm:DescribeParameters` et `ssm:GetParameters` à votre politique. `ssm:DescribeParameters` accorde à vos utilisateurs l'autorisation d'afficher et de sélectionner des paramètres Systems Manager. `ssm:GetParameters` accorde à vos utilisateurs l'autorisation d'obtenir les valeurs des paramètres Systems Manager. Vous pouvez également restreindre l'accès à des paramètres Systems Manager spécifiques. Pour plus d'informations, consultez [Restreindre l'accès à des paramètres Systems Manager spécifiques](#) plus loin dans cette section.

À l'heure actuelle, les actions d'API Amazon EC2 `Describe*` ne prennent pas en charge les autorisations au niveau des ressources, vous ne pouvez donc pas limiter les ressources individuelles que les utilisateurs peuvent afficher dans l'assistant de lancement d'instances. Cependant, vous pouvez appliquer les autorisations au niveau des ressources sur l'action d'API `ec2:RunInstances` pour limiter les ressources que les utilisateurs peuvent employer pour lancer une instance. Le lancement échoue si les utilisateurs sélectionnent des options qu'ils ne sont pas autorisés à utiliser.

Limiter l'accès à un type d'instance, un sous-réseau et une région spécifiques

La stratégie suivante autorise les utilisateurs à lancer les instances `t2.micro` à l'aide des AMI dont Amazon est propriétaire, et uniquement sur un sous-réseau spécifique (`subnet-1a2b3c4d`). Les utilisateurs ne peuvent procéder à un lancement que dans la région `sa-east-1`. Si les utilisateurs sélectionnent une autre région ou un autre type d'instance, d'AMI ou de sous-réseau dans l'assistant de lancement d'instances, le lancement échoue.

La première instruction accorde aux utilisateurs l'autorisation d'afficher les options dans l'assistant de lancement d'instances ou d'en créer de nouvelles, comme illustré dans l'exemple ci-dessus. La deuxième déclaration accorde aux utilisateurs l'autorisation d'utiliser les ressources interface réseau, volume, paire de clés, groupe de sécurité et sous-réseau pour l'action `ec2:RunInstances`, lesquelles sont requises pour lancer une instance sur un VPC. Pour plus d'informations sur l'utilisation de l'action `ec2:RunInstances`, consultez [Instances de lancement \(RunInstances\)](#). Les troisième et quatrième déclarations accordent aux utilisateurs l'autorisation d'utiliser, respectivement, les ressources de l'instance et celles de l'AMI, mais uniquement si l'instance est une instance `t2.micro`, et que l'AMI appartient à Amazon, ou à certains partenaires de confiance et vérifiés.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeInstanceTypes",
      "ec2:DescribeKeyPairs",
      "ec2:CreateKeyPair",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:CreateSecurityGroup",
      "ec2:AuthorizeSecurityGroupIngress"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:sa-east-1:111122223333:network-interface/*",
      "arn:aws:ec2:sa-east-1:111122223333:volume/*",
      "arn:aws:ec2:sa-east-1:111122223333:key-pair/*",

```

```

        "arn:aws:ec2:sa-east-1:111122223333:security-group/*",
        "arn:aws:ec2:sa-east-1:111122223333:subnet/subnet-1a2b3c4d"
    ]
},
{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
        "arn:aws:ec2:sa-east-1:111122223333:instance/*"
    ],
    "Condition": {
        "StringEquals": {
            "ec2:InstanceType": "t2.micro"
        }
    }
},
{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
        "arn:aws:ec2:sa-east-1::image/ami-*"
    ],
    "Condition": {
        "StringEquals": {
            "ec2:Owner": "amazon"
        }
    }
}
]
}

```

Restreindre l'accès à des paramètres Systems Manager spécifiques

La politique suivante accorde l'accès à l'utilisation des paramètres Systems Manager avec un nom spécifique.

La première instruction accorde aux utilisateurs l'autorisation d'afficher les paramètres Systems Manager lors de la sélection d'une AMI dans l'assistant de lancement d'instances. La deuxième instruction accorde aux utilisateurs l'autorisation d'utiliser uniquement les paramètres nommés prod-*

```

{
    "Version": "2012-10-17",

```

```
"Statement": [{
  "Effect": "Allow",
  "Action": [
    "ssm:DescribeParameters"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "ssm:GetParameters"
  ],
  "Resource": "arn:aws:ssm:us-east-2:123456123:parameter/prod-*"
}
]
```

Exemple : Utiliser des groupes de sécurité

Afficher les groupes de sécurité et ajouter ou supprimer des règles

La politique suivante accorde aux utilisateurs l'autorisation d'afficher les groupes de sécurité dans la console Amazon EC2, d'ajouter et de supprimer des règles entrantes et sortantes et de répertorier et modifier des descriptions de règles pour les groupes de sécurité existants ayant l'étiquette `Department=Test`.

Dans la première déclaration, l'action `ec2:DescribeTags` permet aux utilisateurs d'afficher les balises sur la console, ce qui permet aux utilisateurs d'identifier plus facilement les groupes de sécurité qu'ils sont autorisés à modifier.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSecurityGroupRules",
      "ec2:DescribeTags"
    ],
    "Resource": "*"
  },
  {
```

```
"Effect": "Allow",
"Action": [
  "ec2:AuthorizeSecurityGroupIngress",
  "ec2:RevokeSecurityGroupIngress",
  "ec2:AuthorizeSecurityGroupEgress",
  "ec2:RevokeSecurityGroupEgress",
  "ec2:ModifySecurityGroupRules",
  "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
  "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
],
"Resource": [
  "arn:aws:ec2:region:111122223333:security-group/*"
],
"Condition": {
  "StringEquals": {
    "aws:ResourceTag/Department": "Test"
  }
}
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:ModifySecurityGroupRules"
  ],
  "Resource": [
    "arn:aws:ec2:region:111122223333:security-group-rule/*"
  ]
}
]}
```

Utiliser la boîte de dialogue Créer un groupe de sécurité

Vous pouvez créer une stratégie qui permet aux utilisateurs d'utiliser la boîte de dialogue Créer un groupe de sécurité sur la console Amazon EC2. Pour utiliser cette boîte de dialogue, les utilisateurs doivent avoir l'autorisation d'utiliser au moins les actions d'API suivantes :

- `ec2:CreateSecurityGroup` : créer un groupe de sécurité.
- `ec2:DescribeVpcs` : afficher la liste des VPC existants dans la liste VPC.

Avec ces autorisations, les utilisateurs peuvent créer un groupe de sécurité avec succès, mais ne peuvent pas lui ajouter de règles. Pour utiliser les règles dans la boîte de dialogue Créer un groupe de sécurité, vous pouvez ajouter les actions d'API suivantes à votre stratégie :

- `ec2:AuthorizeSecurityGroupIngress` : ajouter des règles entrantes.
- `ec2:AuthorizeSecurityGroupEgress` : ajouter des règles sortantes aux groupes de sécurité VPC.
- `ec2:RevokeSecurityGroupIngress` : modifier ou supprimer des règles entrantes existantes. Cette règle est utile pour permettre aux utilisateurs d'utiliser la fonction Copier vers le nouveau sur la console. Cette fonction ouvre la boîte de dialogue Créer un groupe de sécurité et la complète avec les mêmes règles que le groupe de sécurité sélectionné.
- `ec2:RevokeSecurityGroupEgress` : modifier ou supprimer les règles sortantes pour les groupes de sécurité VPC. Cette règle permet aux utilisateurs de modifier ou de supprimer la règle sortante par défaut qui autorise tout le trafic sortant.
- `ec2>DeleteSecurityGroup` : répondre lorsque les règles non valides ne peuvent pas être enregistrées. La console commence par créer le groupe de sécurité et ajoute ensuite les règles spécifiées. Si les règles ne sont pas valides, l'action échoue et la console tente de supprimer le groupe de sécurité. Comme la boîte de dialogue Créer un groupe de sécurité reste affichée, l'utilisateur peut corriger la règle non valide et essayer de recréer le groupe de sécurité. Cette action d'API n'est pas obligatoire, mais si l'utilisateur n'a pas l'autorisation de l'utiliser et tente de créer un groupe de sécurité avec des règles non valides, le groupe de sécurité est créé sans aucune règle et l'utilisateur doit les ajouter après-coup.
- `ec2:UpdateSecurityGroupRuleDescriptionsIngress` : pour ajouter ou mettre à jour des descriptions des règles de trafic entrant pour les groupes de sécurité.
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress` : pour ajouter ou mettre à jour des descriptions des règles de trafic sortant pour les groupes de sécurité.
- `ec2:ModifySecurityGroupRules` : pour modifier les règles de groupe de sécurité.
- `ec2:DescribeSecurityGroupRules` : pour répertorier les règles de groupe de sécurité.

La stratégie suivante accorde aux utilisateurs l'autorisation d'utiliser la boîte de dialogue Créer un groupe de sécurité, ainsi que de créer des règles entrantes et sortantes pour les groupes de sécurité associés à un VPC spécifique (`vpc-1a2b3c4d`). Les utilisateurs peuvent créer des groupes de sécurité pour un VPC, mais ne peuvent pas leur ajouter de règles. De même, les utilisateurs ne peuvent pas ajouter de règles à un groupe de sécurité qui n'est pas associé au VPC `vpc-1a2b3c4d`. Les utilisateurs reçoivent aussi l'autorisation d'afficher tous les groupes de sécurité sur la console. Les utilisateurs peuvent ainsi identifier plus facilement les groupes de sécurité auxquels ils peuvent ajouter des règles entrantes. Cette stratégie accorde également aux utilisateurs l'autorisation de supprimer les groupes de sécurité associés au VPC `vpc-1a2b3c4d`.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeSecurityGroups",
      "ec2:CreateSecurityGroup",
      "ec2:DescribeVpcs"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2>DeleteSecurityGroup",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress"
    ],
    "Resource": "arn:aws:ec2:region:111122223333:security-group/*",
    "Condition": {
      "ArnEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:111122223333:vpc/vpc-1a2b3c4d"
      }
    }
  }
]
}
```

Exemple : Utiliser des adresses IP Elastic

Pour autoriser les utilisateurs à afficher les adresses IP Elastic sur la console Amazon EC2, vous devez leur accorder l'autorisation d'utiliser l'action `ec2:DescribeAddresses`.

Pour autoriser les utilisateurs à utiliser les adresses IP Elastic, vous pouvez ajouter les actions suivantes à votre politique.

- `ec2:AllocateAddress` : allouer une adresse IP Elastic.
- `ec2:ReleaseAddress`: libérer une adresse IP Elastic.
- `ec2:AssociateAddress` : associer une adresse IP Elastic à une instance ou une interface réseau.

- `ec2:DescribeNetworkInterfaces` et `ec2:DescribeInstances` : utiliser l'écran Associer l'adresse. Cet écran affiche les instances ou interfaces réseau disponibles auxquelles vous pouvez associer une adresse IP Elastic.
- `ec2:DisassociateAddress` : dissocier une adresse IP Elastic d'une instance ou d'une interface réseau.

La politique suivante permet aux utilisateurs d'afficher, d'allouer et d'associer des adresses IP Elastic pour les instances. Les utilisateurs ne peuvent pas associer des adresses IP Elastic à des interfaces réseau, dissocier des adresses IP Elastic ou en libérer.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAddresses",
        "ec2:AllocateAddress",
        "ec2:DescribeInstances",
        "ec2:AssociateAddress"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemple : Utiliser instances réservées

La politique suivante permet aux utilisateurs d'afficher et de modifier les instances réservées de votre compte, ainsi que d'acheter de nouvelles instances réservées dans la AWS Management Console.

Cette politique permet aux utilisateurs d'afficher tous les instances réservées, ainsi que instances à la demande, dans le compte. Il n'est pas possible de définir des autorisations au niveau des ressources pour les instances réservées individuelles.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeReservedInstances",
```

```
    "ec2:ModifyReservedInstances",
    "ec2:PurchaseReservedInstancesOffering",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeReservedInstancesOfferings"
  ],
  "Resource": "*"
}
]
```

L'action `ec2:DescribeAvailabilityZones` est nécessaire pour garantir que la console Amazon EC2 peut afficher des informations sur les zones de disponibilité dans lesquelles vous pouvez acheter des Instances réservées. L'action `ec2:DescribeInstances` n'est pas obligatoire, mais garantit que l'utilisateur peut afficher les instances du compte et acheter des réservations pour correspondre aux spécifications exactes.

Vous pouvez ajuster les actions d'API pour limiter l'accès utilisateur : par exemple, la suppression de `ec2:DescribeInstances` et `ec2:DescribeAvailabilityZones` signifie que l'utilisateur a l'accès en lecture seule.

AWS politiques gérées pour Amazon EC2

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour [créer des politiques gérées par le client IAM](#) qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent les cas d'utilisation courants et sont disponibles dans votre AWS compte. Pour plus d'informations sur les politiques AWS gérées, voir les [politiques AWS gérées](#) dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique `ReadOnlyAccess` d'accès AWS géré fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page [politiques gérées par AWS pour les fonctions de tâche](#) dans le Guide de l'utilisateur IAM.

AWS politique gérée : `AmazonEC2FullAccess`

Vous pouvez associer la politique `AmazonEC2FullAccess` à vos identités IAM. Cette politique accorde des autorisations qui permettent un accès complet à Amazon EC2.

Pour consulter les autorisations associées à cette politique, reportez-vous [AmazonEC2FullAccess](#) à la référence des politiques AWS gérées.

AWS politique gérée : `AmazonEC2ReadOnlyAccess`

Vous pouvez associer la politique `AmazonEC2ReadOnlyAccess` à vos identités IAM. Cette politique accorde des autorisations qui permettent un accès en lecture seule à Amazon EC2.

Pour consulter les autorisations associées à cette politique, reportez-vous [AmazonEC2ReadOnlyAccess](#) à la référence des politiques AWS gérées.

AWS politique gérée : `AWSEC2CapacityReservationFleetRolePolicy`

Cette politique est attachée au rôle lié à un service intitulé `AWSServiceRoleForEC2CapacityReservationFleet` pour autoriser les réserves de capacité à créer, à modifier et à annuler des réserves de capacité en votre nom. Pour plus d'informations, veuillez consulter la rubrique [Rôle lié à un service pour la flotte de réserve de capacité](#).

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSEC2CapacityReservationFleetRolePolicy](#) à la référence des politiques AWS gérées.

AWS politique gérée : `AWSEC2FleetServiceRolePolicy`

Cette stratégie est attachée au rôle lié à un service nommé `AWSServiceRoleForEC2Fleet` pour permettre à la flotte EC2 de demander, de lancer, de résilier et d'étiqueter des instances en votre nom. Pour plus d'informations, consultez [Rôle lié à un service pour flotte EC2](#).

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSEC2FleetServiceRolePolicy](#) à la référence des politiques AWS gérées.

AWS politique gérée : AWSEC2SpotFleetServiceRolePolicy

Cette politique est attachée au rôle lié à un service nommé AWSServiceRoleForEC2SpotFleet pour permettre à la flotte EC2 de lancer et de gérer des instances en votre nom. Pour plus d'informations, consultez [Rôle lié à un service pour un parc d'instances Spot](#).

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSEC2SpotFleetServiceRolePolicy](#) à la référence des politiques AWS gérées.

AWS politique gérée : AWSEC2SpotServiceRolePolicy

Cette politique est attachée au rôle lié à un service nommé AWSServiceRoleForEC2Spot pour permettre à Amazon EC2 de lancer et de gérer des instances Spot en votre nom. Pour plus d'informations, consultez [Rôle lié à un service pour les demandes d'instance Spot](#).

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSEC2SpotServiceRolePolicy](#) à la référence des politiques AWS gérées.

AWS politique gérée : AWSEC2VssSnapshotPolicy

Vous pouvez associer cette politique gérée au rôle de profil d'instance IAM que vous utilisez pour vos instances Windows Amazon EC2. La politique accorde des autorisations permettant à Amazon EC2 de créer et de gérer des instantanés VSS en votre nom.

Pour consulter les autorisations associées à cette politique, reportez-vous [AWSEC2VssSnapshotPolicy](#) à la référence des politiques AWS gérées.

AWS politique gérée : EC2FastLaunchFullAccess

Vous pouvez associer la EC2FastLaunchFullAccess politique à votre profil d'instance ou à un autre rôle IAM. Cette politique accorde un accès complet aux actions EC2 Fast Launch et des autorisations ciblées comme suit.

Détails de l'autorisation

- Lancement rapide EC2 : l'accès administratif est accordé afin que le rôle puisse activer ou désactiver EC2 Fast Launch et décrire les images de lancement rapide EC2.
- Amazon EC2 — L'accès est accordé pour Amazon RunInstances EC2CreateTags , et décrivez les actions nécessaires pour vérifier les autorisations des ressources.

- IAM — L'accès est accordé pour obtenir et utiliser des profils d'instance dont le nom contient `ec2fastlaunch` pour créer le rôle lié au `EC2FastLaunchServiceRolePolicy` service.

Pour consulter les autorisations associées à cette politique, reportez-vous [EC2FastLaunchFullAccess](#) à la référence des politiques AWS gérées.

AWS politique gérée : EC2FastLaunchServiceRolePolicy

Cette politique est attachée au rôle lié au service nommé `AWSServiceRoleForEC2FastLaunch` pour permettre à Amazon EC2 de créer et de gérer un ensemble de snapshots préconfigurés qui réduisent le temps nécessaire au lancement des instances depuis votre AMI compatible EC2 Fast Launch. Pour plus d'informations, consultez [the section called "Rôle lié à un service"](#).

Pour consulter les autorisations associées à cette politique, reportez-vous [EC2FastLaunchServiceRolePolicy](#) à la référence des politiques AWS gérées.

AWS politique gérée : Ec2InstanceConnectEndpoint

Cette politique est attachée à un rôle lié à un service nommé `AWSServiceRoleForEC2InstanceConnect` pour permettre au point de terminaison EC2 Instance Connect d'effectuer des actions en votre nom. Pour plus d'informations, consultez [Rôle lié à un service pour le point de terminaison EC2 Instance Connect](#).

Pour consulter les autorisations associées à cette politique, reportez-vous [Ec2InstanceConnectEndpoint](#) à la référence des politiques AWS gérées.

Mises à jour des politiques gérées par Amazon EC2 AWS

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon EC2 depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
EC2FastLaunchFullAccess : nouvelle politique	Amazon EC2 a ajouté cette politique pour effectuer des actions d'API liées à la fonctionnalité EC2 Fast Launch à partir d'une instance. La politique peut être attachée	14 mai 2024

Modification	Description	Date
	au profil d'instance d'une instance lancée à partir d'une AMI compatible avec EC2 Fast Launch.	
AWSEC2VssSnapshotPolicy : nouvelle politique	Amazon EC2 a ajouté la <code>AWSEC2VssSnapshotPolicy</code> politique qui contient les autorisations permettant de créer et d'ajouter des balises aux Amazon Machine Images (AMI) et aux instantanés EBS.	28 mars 2024
EC2FastLaunchServiceRolePolicy : nouvelle politique	Amazon EC2 a ajouté la fonctionnalité EC2 Fast Launch pour permettre aux AMI Windows de lancer des instances plus rapidement en créant un ensemble de snapshots préprovisionnés.	26 novembre 2021
Amazon EC2 a commencé à assurer le suivi des modifications	Amazon EC2 a commencé à suivre les modifications apportées à ses politiques gérées AWS	1er mars 2021

Rôles IAM pour Amazon EC2

Les applications doivent signer leurs demandes d'API avec des AWS informations d'identification. Par conséquent, si vous êtes un développeur d'applications, vous avez besoin d'une stratégie pour gérer les informations d'identification de vos applications qui s'exécutent sur les instances EC2. Par exemple, vous pouvez distribuer en toute sécurité vos informations d'identification AWS aux instances, en permettant ainsi aux applications de ces instances d'utiliser vos informations d'identification pour signer des demandes, tout en les protégeant des autres utilisateurs. Cependant, il est difficile de distribuer en toute sécurité les informations d'identification à chaque instance,

en particulier celles AWS créées en votre nom, telles que les instances Spot ou les instances de groupes Auto Scaling. Vous devez également être en mesure de mettre à jour les informations d'identification sur chaque instance lorsque vous effectuez une rotation de vos AWS informations d'identification.

Note

Pour vos charges de travail Amazon EC2, nous vous recommandons de récupérer les informations d'identification de session en utilisant la méthode décrite ci-dessous. Ces informations d'identification devraient permettre à votre charge de travail d'effectuer des requêtes d'API AWS, sans avoir besoin d'utiliser `sts:AssumeRole` pour assumer le rôle déjà associé à l'instance. À moins que vous ne deviez transmettre des balises de session pour le contrôle d'accès par attributs (ABAC) ou adopter une politique de session pour restreindre davantage les autorisations du rôle, ces appels de prise en charge de rôle sont inutiles, car ils créent un nouveau jeu des mêmes informations d'identification de session de rôle temporaire.

Si votre charge de travail utilise un rôle pour s'assumer elle-même, vous devez créer une politique de confiance qui autorise explicitement ce rôle à s'assumer lui-même. Si vous ne créez pas la politique de confiance, vous obtenez l'erreur `AccessDenied`. Pour de plus amples informations, veuillez consulter la rubrique [Modifying a role trust policy](#) (Modification d'une politique d'approbation de rôle) dans le Guide de l'utilisateur IAM.

Nous avons conçu les rôles IAM de telle sorte que vos applications puissent créer des demandes d'API en toute sécurité depuis vos instances, sans requérir que vous gériez les informations d'identification de sécurité que les applications utilisent. Au lieu de créer et de distribuer vos AWS informations d'identification, vous pouvez déléguer l'autorisation d'effectuer des demandes d'API à l'aide des rôles IAM comme suit :

1. Créez un rôle IAM.
2. Définissez quels comptes ou AWS services peuvent assumer le rôle.
3. Définissez les actions d'API et les ressources que l'application peut utiliser en assumant le rôle.
4. Spécifiez le rôle au lancement de votre instance ou attachez-le à une instance existante.
5. Demandez à l'application d'extraire un ensemble d'informations d'identification temporaires et utilisez-les.

Par exemple, vous pouvez utiliser des rôles IAM pour accorder l'autorisation aux applications de s'exécuter sur vos instances qui ont besoin d'utiliser un compartiment dans Amazon S3. Vous pouvez spécifier des permissions pour les rôles IAM en créant une politique au format JSON. Ces politiques sont similaires à celles que vous créez pour les utilisateurs. Si vous modifiez un rôle, la modification est répercutée sur toutes les instances.

Note

Les informations d'identification du rôle Amazon EC2 IAM ne sont pas soumises aux durées de session maximales configurées dans le rôle. Pour de plus amples informations, veuillez consulter [Utilisation de rôles IAM](#) dans le Guide de l'utilisateur IAM.

Lors de la création de rôles IAM, associez des politiques IAM de moindres privilèges qui restreignent l'accès aux appels d'API spécifiques requis par l'application. Pour la communication Windows vers Windows, utilisez des groupes et des rôles Windows bien définis et bien documentés pour accorder un accès au niveau de l'application entre les instances Windows. Les groupes et les rôles permettent aux clients de définir des autorisations au niveau des applications à moindre privilège et des dossiers NTFS pour limiter l'accès aux exigences spécifiques de l'application.

Vous ne pouvez attacher qu'un rôle IAM à une instance, mais vous pouvez attacher le même rôle à de nombreuses instances. Pour plus d'informations sur la création et l'utilisation des rôles IAM, consultez [Rôles](#) dans le IAM Guide de l'utilisateur.

Vous pouvez appliquer des autorisations au niveau des ressources à vos politiques IAM pour contrôler la possibilité pour les utilisateurs d'attacher, de remplacer ou de détacher des rôles IAM pour une instance. Pour plus d'informations, consultez [Autorisations au niveau des ressources prises en charge pour les opérations d'API Amazon EC2](#) et l'exemple suivant : [Exemple : Utiliser des rôles IAM](#).

Sommaire

- [Profils d'instance](#)
- [Extraire les informations d'identification de sécurité à partir des métadonnées d'instance](#)
- [Octroi à un utilisateur de l'autorisation de transmettre un rôle IAM à une instance](#)
- [Utiliser les rôles IAM](#)

Profils d'instance

Amazon EC2 utilise un profil d'instance comme conteneur d'un rôle IAM. Lorsque vous créez un rôle IAM à l'aide de la console IAM, celle-ci crée automatiquement un profil d'instance et lui attribue le même nom qu'au rôle auquel il correspond. Si vous utilisez la console Amazon EC2 pour lancer une instance avec un rôle IAM ou pour attacher un rôle IAM à une instance, vous devez choisir le rôle en vous basant sur une liste de noms de profils d'instance.

Si vous utilisez l' AWS CLI API ou un AWS SDK pour créer un rôle, vous créez le rôle et le profil d'instance en tant qu'actions distinctes, avec des noms potentiellement différents. Si vous utilisez ensuite l' AWS CLI API ou un AWS SDK pour lancer une instance avec un rôle IAM ou pour attacher un rôle IAM à une instance, spécifiez le nom du profil d'instance.

Un profil d'instance ne peut contenir qu'un seul rôle IAM. Cette limite ne peut pas être augmentée.

Pour plus d'informations, consultez [Profils d'instance](#) dans le IAM Guide de l'utilisateur.

Extraire les informations d'identification de sécurité à partir des métadonnées d'instance

Une application de l'instance extrait les informations d'identification de sécurité fournies par le rôle à partir de l'élément `iam/security-credentials/nom-rôle` des métadonnées d'instance. L'application reçoit les autorisations pour les actions et les ressources que vous avez définies pour le rôle via les informations d'identification de sécurité associées au rôle. Ces informations de sécurité sont temporaires et nous les faisons tourner automatiquement. Nous rendons disponibles de nouvelles informations d'identification au moins cinq minutes avant l'expiration des anciennes informations d'identification.

Warning

Si vous utilisez des services qui emploient les métadonnées d'instance avec les rôles IAM, assurez-vous de ne pas exposer vos informations d'identification quand les services effectuent des appels HTTP en votre nom. Les types de services qui peuvent exposer vos informations d'identification incluent les proxys HTTP, les services de validation HTML/CSS et les processeurs XML qui prennent en charge l'inclusion XML.

La commande suivante extrait les informations de sécurité pour un rôle IAM intitulé `s3access`.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

Voici un exemple de sortie.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
```

```
}
```

Pour les applications et PowerShell les commandes Tools for Windows qui s'exécutent sur l'instance, il n'est pas nécessaire d'obtenir explicitement les informations d'identification de sécurité temporaires : AWS les SDK et les outils pour Windows obtiennent PowerShell automatiquement les informations d'identification du service de métadonnées d'instance EC2 et les utilisent. AWS CLI AWS CLI Pour effectuer un appel en dehors de l'instance à l'aide d'informations d'identification de sécurité temporaires (par exemple, pour tester les politiques IAM), vous devez fournir la clé d'accès, la clé secrète et le jeton de session. Pour plus d'informations, consultez la section [Utilisation d'informations d'identification de sécurité temporaires pour demander l'accès aux AWS ressources](#) dans le guide de l'utilisateur IAM.

Pour obtenir plus d'informations sur les métadonnées d'instance, consultez [Utiliser des métadonnées d'instance](#). Pour plus d'informations sur l'adresse IP des métadonnées d'instance, consultez [Récupérer des métadonnées d'instance](#).

Octroi à un utilisateur de l'autorisation de transmettre un rôle IAM à une instance

Pour permettre à un utilisateur de lancer une instance avec un rôle IAM, ou d'attacher ou remplacer un rôle IAM pour une instance existante, vous devez accorder à l'utilisateur l'autorisation d'utiliser les actions d'API suivantes :

- iam:PassRole
- ec2:AssociateIamInstanceProfile
- ec2:ReplaceIamInstanceProfileAssociation

Par exemple, la politique IAM suivante accorde aux utilisateurs l'autorisation de lancer des instances avec un rôle IAM, ou d'attacher ou remplacer un rôle IAM pour une instance existante à l'aide de la AWS CLI.

Note

Si vous voulez que la politique accorde aux utilisateurs l'accès à tous vos rôles, spécifiez la ressource comme * dans la politique. Cependant, veuillez considérer le principe du [moindre privilège](#) comme une bonne pratique.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "ec2:RunInstances",
      "ec2:AssociateIamInstanceProfile",
      "ec2:ReplaceIamInstanceProfileAssociation"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
  }
]
```

Pour autoriser les utilisateurs à lancer des instances avec un rôle IAM, ou à attacher ou remplacer un rôle IAM pour une instance existante, à l'aide de la console Amazon EC2, vous devez leur accorder l'autorisation d'utiliser `iam:ListInstanceProfiles`, `iam:PassRole`, `ec2:AssociateIamInstanceProfile`, et `ec2:ReplaceIamInstanceProfileAssociation` en plus de toutes les autres autorisations dont ils pourraient avoir besoin. Pour obtenir des exemples de politiques, consultez [Exemples de politiques à utiliser sur la console Amazon EC2](#).

Utiliser les rôles IAM

Vous pouvez créer un rôle IAM et l'attacher à une instance pendant ou après le lancement. Vous pouvez aussi remplacer ou détacher un rôle IAM pour une instance.

Sommaire

- [créer un rôle IAM](#) ;
- [Lancer une instance avec un rôle IAM](#)
- [Attacher un rôle IAM à une instance](#)
- [Remplacer un rôle IAM](#)
- [Détacher un rôle IAM](#)
- [Générer une politique pour votre rôle IAM en fonction de l'activité d'accès](#)

créer un rôle IAM ;

Vous devez créer un rôle IAM avant de pouvoir lancer une instance avec ce rôle ou attacher celui-ci à une instance.

Console

Pour créer un rôle IAM avec la console IAM

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Rôles, puis Créer un rôle.
3. Sur la page Sélectionner une entité sécurisée, choisissez Service AWS, puis sélectionnez le cas d'utilisation EC2. Choisissez Suivant.
4. Sur la page Ajouter des autorisations, sélectionnez les politiques qui accordent à vos instances l'accès aux ressources dont elles ont besoin. Choisissez Suivant.
5. Sur la page Nommer, vérifier et créer, saisissez un nom et une description pour le rôle. Vous pouvez également ajouter des balises au rôle. Sélectionnez Créer un rôle.

Command line

L'exemple suivant crée un rôle IAM avec une politique qui lui permet d'utiliser un compartiment Amazon S3.

Pour créer un rôle IAM et un profil d'instance (AWS CLI)

1. Créez la stratégie d'approbation suivante et enregistrez-la dans un fichier texte intitulé `ec2-role-trust-policy.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com" },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Créez le rôle `s3access` et spécifiez la stratégie d'approbation que vous avez créée à l'aide de la commande `create-role`.

```
aws iam create-role \  
  --role-name s3access \  
  --assume-role-policy-document file://ec2-role-trust-policy.json
```

Exemple de réponse

```
{  
  "Role": {  
    "AssumeRolePolicyDocument": {  
      "Version": "2012-10-17",  
      "Statement": [  
        {  
          "Action": "sts:AssumeRole",  
          "Effect": "Allow",  
          "Principal": {  
            "Service": "ec2.amazonaws.com"  
          }  
        }  
      ]  
    },  
    "RoleId": "AR0AIIIZKPBKS2LEXAMPLE",  
    "CreateDate": "2013-12-12T23:46:37.247Z",  
    "RoleName": "s3access",  
    "Path": "/",  
    "Arn": "arn:aws:iam::123456789012:role/s3access"  
  }  
}
```

3. Créez une stratégie d'accès et enregistrez-la dans un fichier texte intitulé `ec2-role-access-policy.json`. Par exemple, cette politique d'accès accorde des permissions administratives pour Amazon S3 aux applications s'exécutant sur l'instance.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": ["s3:*"],  
      "Resource": ["*"]  
    }  
  ]  
}
```

```
    }  
  ]  
}
```

4. Attachez la stratégie d'accès au rôle à l'aide de la commande [put-role-policy](#).

```
aws iam put-role-policy \  
  --role-name s3access \  
  --policy-name S3-Permissions \  
  --policy-document file://ec2-role-access-policy.json
```

5. Créez un profil d'instance nommé `s3access-profile` à l'aide de la commande [create-instance-profile](#).

```
aws iam create-instance-profile --instance-profile-name s3access-profile
```

Exemple de réponse

```
{  
  "InstanceProfile": {  
    "InstanceProfileId": "AIPAJTLBPJLEGREXAMPLE",  
    "Roles": [],  
    "CreateDate": "2013-12-12T23:53:34.093Z",  
    "InstanceProfileName": "s3access-profile",  
    "Path": "/",  
    "Arn": "arn:aws:iam::123456789012:instance-profile/s3access-profile"  
  }  
}
```

6. Ajoutez le rôle `s3access` au profil d'instance `s3access-profile`.

```
aws iam add-role-to-instance-profile \  
  --instance-profile-name s3access-profile \  
  --role-name s3access
```

Vous pouvez également utiliser les AWS Tools for Windows PowerShell commandes suivantes :

- [New-IAMRole](#)
- [S'inscrire - IAM RolePolicy](#)
- [Nouveau IAM InstanceProfile](#)

Lancer une instance avec un rôle IAM

Après avoir créé un rôle IAM, vous pouvez lancer une instance et associer le rôle à l'instance durant le lancement.

Important

Après que vous avez créé un rôle IAM, la propagation des permissions peut prendre plusieurs secondes. En cas d'échec de votre première tentative de lancer une instance avec un rôle, attendez quelques secondes avant de recommencer. Pour plus d'informations, consultez [Résolution des problèmes liés aux rôles IAM](#) dans le guide de l'utilisateur IAM.

New console

Pour lancer une instance avec un rôle IAM (console)

1. Suivez la procédure pour [lancer une instance](#).
2. Développez Advanced details (Détails avancés), et pour IAM instance profile (Profil d'instance IAM), sélectionnez le rôle IAM que vous avez créé.

Note

La liste IAM instance profile (Profil d'instance IAM) affiche le nom du profil d'instance que vous avez créé lorsque vous avez créé votre rôle IAM. Si vous avez créé votre rôle IAM à l'aide de la console, le profil d'instance a été créé automatiquement et reçu le même nom que le rôle. Si vous avez créé votre rôle IAM à l'AWS CLI aide de l'API ou d'un AWS SDK, vous avez peut-être nommé votre profil d'instance différemment.

3. Configurez tous les autres détails dont vous avez besoin pour votre instance ou acceptez les valeurs par défaut, puis sélectionnez une paire de clés. Pour plus d'informations sur les champs de l'assistant de lancement d'instance, consultez [Lancer une instance à l'aide de paramètres définis](#).
4. Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance).
5. Si vous utilisez les actions de l'API Amazon EC2 dans votre application, récupérez les informations d'identification AWS de sécurité mises à disposition sur l'instance et utilisez-les pour signer les demandes. Le AWS SDK le fait pour vous.

IMDSv2

Pour les instances Linux, consultez l'exemple suivant :

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
  "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/iam/security-credentials/role_name
```

Pour les instances Windows, consultez l'exemple suivant :

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-
ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
-Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

IMDSv1

Pour les instances Linux, consultez l'exemple suivant :

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

Pour les instances Windows, consultez l'exemple suivant :

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/
security-credentials/role_name
```

Old console

Pour lancer une instance avec un rôle IAM (console)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sur le tableau de bord, choisissez Lancer une instance.

3. Sélectionnez une AMI et un type d'instance et choisissez ensuite Next: Configure Instance Details (Suivant : Configurer les détails de l'instance).
4. Sur la page Configurer les détails de l'instance, pour Rôle IAM, sélectionnez le rôle IAM que vous avez créé.

 Note

La liste Rôle IAM affiche le nom du profil d'instance que vous avez créé lorsque vous avez créé votre rôle IAM. Si vous avez créé votre rôle IAM à l'aide de la console, le profil d'instance a été créé automatiquement et reçu le même nom que le rôle. Si vous avez créé votre rôle IAM à l'aide de l'AWS CLI, de l'API ou d'un AWS SDK, vous avez peut-être nommé votre profil d'instance différemment.

5. Configurez les autres détails, puis suivez les déclarations restantes de l'assistant, ou choisissez Vérifier et lancer pour accepter les paramètres par défaut et accéder directement à la page Examiner le lancement de l'instance.
6. Vérifiez vos paramètres, puis sélectionnez Lancer pour choisir une paire de clés et démarrer votre instance.
7. Si vous utilisez les actions de l'API Amazon EC2 dans votre application, récupérez les informations d'identification AWS de sécurité mises à disposition sur l'instance et utilisez-les pour signer les demandes. Le AWS SDK le fait pour vous.

IMDSv2

Pour les instances Linux, consultez l'exemple suivant :

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Pour les instances Windows, consultez l'exemple suivant :

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
-Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

IMDSv1

Pour les instances Linux, consultez l'exemple suivant :

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

Pour les instances Windows, consultez l'exemple suivant :

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/
security-credentials/role_name
```

Command line

Vous pouvez utiliser le AWS CLI pour associer un rôle à une instance lors du lancement. Vous devez spécifier le profil d'instance dans la commande.

Pour lancer une instance avec un rôle IAM (AWS CLI)

1. Utilisez la commande [run-instances](#) pour lancer une instance à l'aide du profil d'instance. L'exemple suivant montre comment lancer une instance avec le profil d'instance.

```
aws ec2 run-instances \  
  --image-id ami-11aa22bb \  
  --iam-instance-profile Name="s3access-profile" \  
  --key-name my-key-pair \  
  --security-groups my-security-group \  
  --subnet-id subnet-1a2b3c4d
```

Vous pouvez également utiliser la PowerShell commande [New-EC2InstanceOutils](#) pour Windows.

2. Si vous utilisez les actions de l'API Amazon EC2 dans votre application, récupérez les informations d'identification AWS de sécurité mises à disposition sur l'instance et utilisez-les pour signer les demandes. Le AWS SDK le fait pour vous.

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Attacher un rôle IAM à une instance

Pour attacher un IAM à une instance qui n'a pas de rôle, l'instance doit être en état `stopped` ou `running`.

Console

Pour attacher un rôle IAM à une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis Actions, Security (Sécurité), Modify IAM role (Modifier le rôle IAM).
4. Sélectionnez le rôle IAM à attacher à votre instance et choisissez Save (Enregistrer).

Command line

Pour attacher un rôle IAM à une instance (AWS CLI)

1. Si nécessaire, décrivez vos instances pour obtenir l'ID de l'instance à laquelle attacher le rôle.

```
aws ec2 describe-instances
```

2. Utilisez la commande [associate-iam-instance-profile](#) pour attacher le rôle IAM à l'instance en spécifiant le profil d'instance. Vous pouvez utiliser l'Amazon Resource Name (ARN) du profil d'instance ou le nom du profil d'instance.

```
aws ec2 associate-iam-instance-profile \  
  --instance-id i-1234567890abcdef0 \  
  --iam-instance-profile Name="TestRole-1"
```

Exemple de réponse

```
{  
  "IamInstanceProfileAssociation": {
```

```
"InstanceId": "i-1234567890abcdef0",
"State": "associating",
"AssociationId": "iip-assoc-0dbd8529a48294120",
"IamInstanceProfile": {
  "Id": "AIPAJLNLDX3AMYZWNWYYAY",
  "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-1"
}
}
```

Vous pouvez également utiliser les PowerShell commandes Outils pour Windows suivantes :

- [Get-EC2Instance](#)
- [Register-EC2IamInstanceProfile](#)

Remplacer un rôle IAM

Pour remplacer le rôle IAM sur une instance qui a déjà un rôle IAM, l'instance doit être en état `running`. Vous pouvez le faire si vous souhaitez modifier le rôle IAM pour une instance sans commencer par détacher le rôle existant. Pour exemple, vous pouvez le faire pour veiller à ce que les actions d'API effectuées par les applications exécutées sur l'instance ne soient pas interrompues.

Console

Pour remplacer un rôle IAM pour une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis Actions, Security (Sécurité), Modify IAM role (Modifier le rôle IAM).
4. Sélectionnez le rôle IAM à attacher à votre instance et choisissez Save (Enregistrer).

Command line

Pour remplacer un rôle IAM pour une instance (AWS CLI)

1. Si nécessaire, décrivez vos associations de profils d'instance IAM pour obtenir l'ID d'association du profil d'instance IAM à remplacer.

```
aws ec2 describe-iam-instance-profile-associations
```

2. Utilisez la commande [replace-iam-instance-profile-association](#) pour remplacer le profil d'instance IAM en spécifiant l'ID d'association du profil d'instance existant et l'ARN ou le nom du profil d'instance qui doit le remplacer.

```
aws ec2 replace-iam-instance-profile-association \  
  --association-id iip-assoc-0044d817db6c0a4ba \  
  --iam-instance-profile Name="TestRole-2"
```

Exemple de réponse

```
{  
  "IamInstanceProfileAssociation": {  
    "InstanceId": "i-087711ddaf98f9489",  
    "State": "associating",  
    "AssociationId": "iip-assoc-09654be48e33b91e0",  
    "IamInstanceProfile": {  
      "Id": "AIPAJCJEDKX7QYHWYK7GS",  
      "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"  
    }  
  }  
}
```

Vous pouvez également utiliser les PowerShell commandes Outils pour Windows suivantes :

- [Get-EC2IamInstanceProfileAssociation](#)
- [Set-EC2IamInstanceProfileAssociation](#)

Détacher un rôle IAM

Vous ne pouvez pas détacher un rôle IAM d'une instance en cours d'exécution ou arrêtée.

Console

Pour détacher un rôle IAM d'une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance, puis Actions, Security (Sécurité), Modify IAM role (Modifier le rôle IAM).
4. Pour IAM role (Rôle IAM), choisissez No IAM Role (Aucun rôle IAM). Choisissez Enregistrer.
5. Dans la boîte de dialogue de confirmation, entrez Detach (Détacher), puis choisissez Detach (Détacher).

Command line

Pour détacher un rôle IAM d'une instance (AWS CLI)

1. Si nécessaire, utilisez [describe-iam-instance-profile-associations](#) pour décrire vos associations de profils d'instance IAM et obtenir l'ID d'association pour le profil d'instance IAM à détacher.

```
aws ec2 describe-iam-instance-profile-associations
```

Exemple de réponse

```
{
  "IamInstanceProfileAssociations": [
    {
      "InstanceId": "i-088ce778fbfeb4361",
      "State": "associated",
      "AssociationId": "iip-assoc-0044d817db6c0a4ba",
      "IamInstanceProfile": {
        "Id": "AIPAJEDNCAA64SSD265D6",
        "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
      }
    }
  ]
}
```

2. Utilisez la commande [disassociate-iam-instance-profile](#) pour détacher le profil d'instance IAM en utilisant son ID d'association.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-  
assoc-0044d817db6c0a4ba
```

Exemple de réponse

```
{
  "IamInstanceProfileAssociation": {
    "InstanceId": "i-087711ddaf98f9489",
    "State": "disassociating",
    "AssociationId": "iip-assoc-0044d817db6c0a4ba",
    "IamInstanceProfile": {
      "Id": "AIPAJEDNCAA64SSD265D6",
      "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
    }
  }
}
```

Vous pouvez également utiliser les PowerShell commandes Outils pour Windows suivantes :

- [Get-EC2IamInstanceProfileAssociation](#)
- [Unregister-EC2IamInstanceProfile](#)

Générer une politique pour votre rôle IAM en fonction de l'activité d'accès

Lorsque vous créez un rôle IAM pour vos applications, vous pouvez parfois accorder plus d'autorisations que nécessaire. Avant de lancer votre application dans votre environnement de production, vous pouvez générer une politique IAM basée sur l'activité d'accès pour un rôle IAM. IAM Access Analyzer examine vos AWS CloudTrail journaux et génère un modèle de politique contenant les autorisations utilisées par le rôle dans la plage de dates spécifiée. Vous pouvez utiliser le modèle pour créer une politique gérée avec des autorisations affinées, puis l'attacher au rôle IAM. Ainsi, vous accordez uniquement les autorisations dont le rôle a besoin pour interagir avec les AWS ressources correspondant à votre cas d'utilisation spécifique. Cela vous permet de mieux respecter la bonne pratique qui consiste à [appliquer le principe du moindre privilège](#). Pour en savoir plus, consultez [Générer des stratégies basées sur l'activité d'accès](#) dans le Guide IAM de l'utilisateur.

Accéder à Amazon EC2 à l'aide du point de terminaison d'un VPC d'interface

Vous pouvez améliorer la posture de sécurité de votre VPC en créant une connexion privée entre votre VPC et Amazon EC2. Vous pouvez accéder à Amazon EC2 comme s'il se trouvait dans

vosre VPC, sans passer par une passerelle Internet, un appareil NAT, une connexion VPN ou une connexion. AWS Direct Connect Les instances de votre VPC ne nécessitent pas d'adresses IP publiques pour accéder à Amazon EC2.

Pour plus d'informations, consultez la section [Accès Services AWS par AWS PrivateLink le biais du AWS PrivateLink guide](#).

Table des matières

- [Création d'un point de terminaison d'un VPC d'interface](#)
- [Créer une politique de point de terminaison](#)

Création d'un point de terminaison d'un VPC d'interface

Création d'un point de terminaison d'interface pour Amazon EC2 à l'aide du nom de service suivant :

- `com.amazonaws.region.ec2` : crée un point de terminaison pour les actions d'API Amazon EC2.

Pour plus d'informations, consultez la section [Accès et Service AWS utilisation d'un point de terminaison VPC d'interface](#) dans le AWS PrivateLink Guide.

Créer une politique de point de terminaison

Une politique de point de terminaison est une ressource IAM que vous pouvez attacher à votre point de terminaison d'interface. La politique de point de terminaison par défaut autorise un accès complet à l'API Amazon EC2 via le point de terminaison d'interface. Pour contrôler l'accès autorisé à l'API Amazon EC2 depuis votre VPC, attachez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Le mandataire qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

⚠ Important

Lorsqu'une politique autre que celle par défaut est appliquée à un point de terminaison VPC d'interface pour Amazon EC2, certaines demandes d'API ayant échoué, telles que celles RequestLimitExceeded provenant de, peuvent ne pas être connectées à Amazon ou à Amazon. AWS CloudTrail CloudWatch

Pour plus d'informations, consultez [Contrôle de l'accès aux services à l'aide de politiques de point de terminaison](#) dans le Guide AWS PrivateLink .

L'exemple suivant illustre une politique de point de terminaison d'un VPC qui refuse l'autorisation de créer des volumes non chiffrés ou de lancer des instances avec des volumes non chiffrés. L'exemple de politique accorde également à tout le monde l'autorisation d'effectuer toutes les autres actions Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "ec2:*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": [
        "ec2:CreateVolume"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Principal": "*",
      "Condition": {
        "Bool": {
          "ec2:Encrypted": "false"
        }
      }
    },
    {
      "Action": [
        "ec2:RunInstances"
      ]
```

```
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Principal": "*",
    "Condition": {
      "Bool": {
        "ec2:Encrypted": "false"
      }
    }
  }
}
```

Gestion des mises à jour pour les instances Windows Amazon EC2

Nous vous recommandons d'appliquer les correctifs, de procéder aux mises à jours et de sécuriser le système d'exploitation et les applications sur vos instances EC2 régulièrement. Vous pouvez utiliser le [Gestionnaire de correctifs AWS Systems Manager](#) pour automatiser le processus d'installation des mises à jour de sécurité pour le système d'exploitation et les applications.

Pour les instances EC2 appartenant à un groupe Auto Scaling, vous pouvez utiliser le runbook [AWS-PatchAsgInstance](#) pour éviter le remplacement des instances faisant l'objet d'un correctif. Vous pouvez aussi utiliser n'importe quel service de mise à jour automatique ou processus recommandé pour l'installation des mises à jour fourni par le fournisseur de l'application.

Ressources

- AL2023 — [Mise à jour de la norme AL2023](#) dans le guide de l'utilisateur Amazon Linux 2023.
- AL2 — [Gérez le logiciel sur votre instance Amazon Linux 2](#) dans le guide de l'utilisateur Amazon Linux 2.
- Instances Windows — [the section called “Gestion des mises à jour”](#).

Bonnes pratiques de sécurité pour les instances Windows

Nous vous recommandons de suivre ces bonnes pratiques de sécurité pour vos instances Windows.

Table des matières

- [Bonnes pratiques de sécurité de haut niveau](#)
- [Gestion des mises à jour](#)

- [Gestion de la configuration](#)
- [Gestion des modifications](#)
- [Audit et responsabilité pour les instances Windows Amazon EC2](#)

Bonnes pratiques de sécurité de haut niveau

Vous devez respecter les meilleures pratiques de sécurité de haut niveau suivantes pour vos instances Windows :

- **Accès minimal** : accordez l'accès uniquement aux systèmes et aux emplacements fiables et attendus. Cela s'applique à tous les produits Microsoft tels que Active Directory, les serveurs de productivité professionnelle Microsoft et les services d'infrastructure, notamment les services de Bureau à distance, les serveurs proxy inversés, les serveurs Web IIS, etc. Utilisez AWS des fonctionnalités telles que les groupes de sécurité des instances Amazon EC2, les listes de contrôle d'accès réseau (ACL) et les sous-réseaux publics/privés Amazon VPC pour renforcer la sécurité sur plusieurs sites d'une architecture. Au sein d'une instance Windows, les clients peuvent utiliser le pare-feu Windows pour renforcer defense-in-depth la stratégie de leur déploiement. Installez uniquement les composants du système d'exploitation et les applications nécessaires au fonctionnement du système aux fins pour lesquelles il a été conçu. Configurez les services d'infrastructure, notamment IIS, pour qu'ils s'exécutent sous des comptes de service ou pour utiliser des fonctionnalités telles que les identités de groupe d'applications pour accéder aux ressources localement et à distance dans votre infrastructure.
- **Privilège minimal** : déterminez l'ensemble minimal de privilèges dont les instances et les comptes ont besoin pour exécuter leurs fonctions. Restreindre ces serveurs et utilisateurs pour autoriser uniquement ces autorisations définies. Utilisez des techniques telles que les contrôles d'accès basés sur les rôles pour réduire la surface des comptes d'administration et créer les rôles les plus limités pour accomplir une tâche. Utilisez les fonctionnalités du système d'exploitation telles que le système de cryptage de fichiers EFS (Encrypting File System) dans NTFS pour chiffrer les données sensibles au repos et contrôler l'accès de l'application et de l'utilisateur à ces dernières.
- **Gestion de la configuration** : créez une configuration de serveur de base qui intègre des correctifs de up-to-date sécurité et des suites de protection basées sur l'hôte, notamment des solutions antivirus, anti-programmes malveillants, détection/prévention des intrusions et surveillance de l'intégrité des fichiers. Évaluez chaque serveur par rapport à la référence enregistrée actuelle pour identifier et signaler les écarts éventuels. Assurez-vous que chaque serveur est configuré pour générer et stocker en toute sécurité les données de journal et d'audit appropriées.

- **Gestion des modifications** : créez des processus pour contrôler les modifications apportées aux lignes de base de configuration des serveurs et optez pour des processus de modification entièrement automatisés. Tirez également parti de Just Enough Administration (JEA) avec Windows PowerShell DSC pour limiter l'accès administratif aux fonctions minimales requises.
- **Gestion des correctifs** : mettez en œuvre des processus qui corrigent, mettent à jour et sécurisent régulièrement le système d'exploitation et les applications sur vos instances EC2.
- **Journaux d'audit** : auditez l'accès et toutes les modifications apportées aux instances Amazon EC2 afin de vérifier l'intégrité du serveur et de vous assurer que seules les modifications autorisées sont apportées. Tirez parti de fonctionnalités telles que la [journalisation améliorée pour IIS](#) afin d'améliorer les fonctionnalités de journalisation par défaut. AWS des fonctionnalités telles que les journaux de flux VPC AWS CloudTrail sont également disponibles pour auditer l'accès au réseau, y compris les demandes autorisées/refusées et les appels d'API, respectivement.

Gestion des mises à jour

Pour garantir les meilleurs résultats lorsque vous exécutez Windows Server sur Amazon EC2, nous vous recommandons de mettre en œuvre les meilleures pratiques suivantes :

- [Configure Windows Update](#)
- [Update drivers](#)
- [Use the latest Windows AMIs](#)
- [Test performance before migration](#)
- [Update launch agents](#)
- Redémarrez votre instance Windows après avoir installé les mises à jour. Pour plus d'informations, consultez [Redémarrer votre instance](#).

Pour savoir comment mettre à niveau ou migrer une instance Windows vers une version plus récente de Windows Server, voir [Mettre à niveau une instance Amazon EC2 Windows vers une nouvelle version de Windows Server](#).

Configuration de Windows Update

Par défaut, les instances lancées à partir d'AMI AWS Windows Server ne reçoivent pas de mises à jour via Windows Update.

Mettre à jour les pilotes Windows

Faites en sorte que les pilotes soient à jour sur toutes les instances EC2 Windows afin d'appliquer les correctifs de problèmes et les améliorations de performances les plus récents à l'échelle de votre flotte d'instances. En fonction de votre type d'instance, vous devez mettre à jour les pilotes AWS PV, Amazon ENA et AWS NVMe.

- Utilisez les [rubriques SNS](#) afin de recevoir les mises à jour des nouvelles versions de pilotes.
- [Utilisez le manuel AWS Systems Manager d'automatisation AWSSupport pour appliquer facilement UpgradeWindows AWSDrivers les mises à jour à toutes vos instances.](#)

Lancer des instances à l'aide des dernières AMI Windows

AWS publie chaque mois de nouvelles AMI Windows, qui contiennent les derniers correctifs, pilotes et agents de lancement du système d'exploitation. Utilisez l'AMI la plus récente lorsque vous lancez de nouvelles instances ou que vous créez vos propres images personnalisées.

- Pour consulter les mises à jour de chaque version des AMI AWS Windows, consultez [l'historique des versions des AMI AWS Windows](#).
- Afin d'utiliser les AMI les plus récentes disponibles, consultez [Requête portant sur la dernière AMI Windows à l'aide de Systems Manager Parameter Store](#).
- Pour plus d'informations sur les AMI Windows spécialisées que vous pouvez utiliser pour lancer des instances pour votre base de données et sur les cas d'utilisation visant à renforcer la conformité, consultez la section [AMI Windows spécialisées](#) dans le manuel de référence des AMI AWS Windows.

Tester les performances du système/des applications avant la migration

La migration des applications d'entreprise vers AWS peut impliquer de nombreuses variables et configurations. Il convient de toujours tester les performances de la solution EC2 afin de vous assurer ce qui suit :

- Les types d'instances sont correctement configurés, y compris la taille des instances, la mise en réseau améliorée et la location (partagée ou dédiée).
- La topologie des instances est appropriée pour la charge de travail et exploite si nécessaire les fonctions hautes performances, telles que la location dédiée, les groupes de placement, les volumes de stockage d'instance et le matériel nu.

Mise à jour des agents de lancement

Effectuez une mise à jour vers la dernière version de l'agent EC2Launch v2 pour vous assurer que les dernières améliorations sont appliquées à l'ensemble de votre flotte. Pour plus d'informations, consultez [the section called "Migrer"](#).

Si vous disposez d'une flotte mixte, ou si vous voulez continuer à utiliser les agents EC2Launch (Windows Server 2016 et 2019) ou EC2 Config (système d'exploitation hérité uniquement), mettez à jour vers les dernières versions des agents respectifs.

Les mises à jour automatiques sont prises en charge sur les combinaisons suivantes de version de Windows Server et d'agents de lancement. Vous pouvez opter pour les mises à jour automatiques dans la console [SSM Quick Setup Host Management](#) sous Agents de lancement Amazon EC2.

Version Windows	EC2Launch v1	EC2Launch v2
2016	✓	✓
2019	✓	✓
2022		✓

- Pour plus d'informations sur la mise à jour vers EC2Launch v2, consultez. [the section called "Installation"](#)
- Pour plus d'informations sur la mise à jour manuelle d'EC2Config, consultez. [the section called "Installer EC2Config"](#)
- Pour plus d'informations sur la mise à jour manuelle d'EC2Launch, consultez. [the section called "Installer EC2Launch"](#)

Gestion de la configuration

Amazon Machine Images (AMI) fournit une configuration initiale pour une instance Amazon EC2, qui inclut le système d'exploitation Windows et les personnalisations facultatives spécifiques au client, notamment les applications et les contrôles de sécurité. Créez un catalogue AMI contenant des lignes de base de configuration de sécurité personnalisées pour garantir que toutes les instances Windows sont lancées avec des contrôles de sécurité standard. Les bases de sécurité peuvent être intégrées dans une AMI, amorcées dynamiquement lors du lancement d'une instance EC2 ou packagées sous

forme de produit pour une distribution uniforme via les portefeuilles Service Catalog AWS . Pour plus d'informations sur la sécurisation d'une AMI, consultez [Bonnes pratiques de création d'AMI](#).

Chaque instance Amazon EC2 doit respecter les normes de sécurité de l'organisation. N'installez pas de rôles et de fonctionnalités Windows qui ne sont pas requis, et installez des logiciels pour vous protéger contre les codes malveillants (antivirus, antimalware, réduction de l'exploitation), surveiller l'intégrité de l'hôte et effectuer la détection des intrusions. Configurez le logiciel de sécurité pour surveiller et maintenir les paramètres de sécurité du système d'exploitation, protéger l'intégrité des fichiers critiques de ce dernier et signaler les écarts par rapport à la référence de sécurité. Envisagez de mettre en œuvre les benchmarks de configuration de sécurité recommandés publiés par Microsoft, le Center for Internet Security (CIS) ou le National Institute of Standards and Technology (NIST). Pensez à utiliser d'autres outils Microsoft pour des serveurs d'applications particuliers, tels que [Best Practice Analyzer for SQL Server](#).

AWS les clients peuvent également exécuter des évaluations Amazon Inspector afin d'améliorer la sécurité et la conformité des applications déployées sur des instances Amazon EC2. Amazon Inspector évalue automatiquement les applications à la recherche de vulnérabilités ou d'écarts par rapport aux bonnes pratiques et inclut une base de connaissances de centaines de règles mappées aux normes de conformité de sécurité communes (par exemple, PCI DSS) et aux définitions de vulnérabilité. Les règles préintégréées prévoient, par exemple, la vérification de l'activation de la connexion distante à la racine ou la détection des versions de logiciels vulnérables installées. Ces règles sont régulièrement mises à jour par les chercheurs en AWS sécurité.

Lors de la sécurisation des instances Windows, nous vous recommandons d'implémenter les services de domaine Active Directory afin d'activer une infrastructure évolutive, sécurisée et gérable pour les emplacements distribués. En outre, après avoir lancé des instances depuis la console Amazon EC2 ou à l'aide d'un outil de provisionnement Amazon EC2, il est recommandé d'utiliser les fonctionnalités natives du système d'exploitation, telles que [Microsoft PowerShell Windows DSC](#), pour maintenir l'état de configuration en cas de dérive de configuration. AWS CloudFormation

Gestion des modifications

Une fois les références de sécurité initiales appliquées aux instances Amazon EC2 au lancement, contrôlez les modifications d'Amazon EC2 en cours pour maintenir la sécurité de vos machines virtuelles. Établissez un processus de gestion des modifications pour autoriser et intégrer les modifications apportées aux AWS ressources (telles que les groupes de sécurité, les tables de routage et les ACL réseau) ainsi qu'aux configurations des systèmes d'exploitation et des applications

(telles que Windows ou l'application de correctifs, les mises à niveau logicielles ou les mises à jour des fichiers de configuration).

AWS fournit plusieurs outils pour aider à gérer les modifications apportées aux AWS ressources AWS CloudTrail, notamment AWS Config AWS CloudFormation, AWS Elastic Beanstalk AWS OpsWorks, et des packs d'administration pour Systems Center Operations Manager et System Center Virtual Machine Manager. Notez que Microsoft publie des correctifs Windows tous les mardis (parfois même tous les jours) et AWS met à jour toutes les AMI Windows gérées dans les cinq jours AWS suivant la publication d'un correctif par Microsoft. Il est donc important de patcher en permanence toutes les AMI de base, de mettre à jour les AWS CloudFormation modèles et les configurations de groupe Auto Scaling avec les derniers ID d'AMI, et de mettre en œuvre des outils pour automatiser la gestion des correctifs d'instance en cours d'exécution.

Microsoft fournit plusieurs options pour gérer les modifications du système d'exploitation Windows et des applications. SCCM, par exemple, fournit une couverture complète du cycle de vie des modifications de l'environnement. Sélectionnez des outils qui répondent aux exigences de l'entreprise et contrôlez la manière dont les modifications affecteront les SLA des applications, la capacité, la sécurité et les procédures de reprise après sinistre. Évitez les modifications manuelles et utilisez plutôt un logiciel de gestion de configuration automatique ou des outils de ligne de commande tels que EC2 Run Command ou Windows PowerShell pour mettre en œuvre des processus de modification scriptés et répétables. Pour répondre à cette exigence, utilisez des hôtes bastion avec journalisation améliorée pour toutes les interactions avec vos instances Windows, afin de vous assurer que tous les événements et toutes les tâches sont automatiquement enregistrés.

Audit et responsabilité pour les instances Windows Amazon EC2

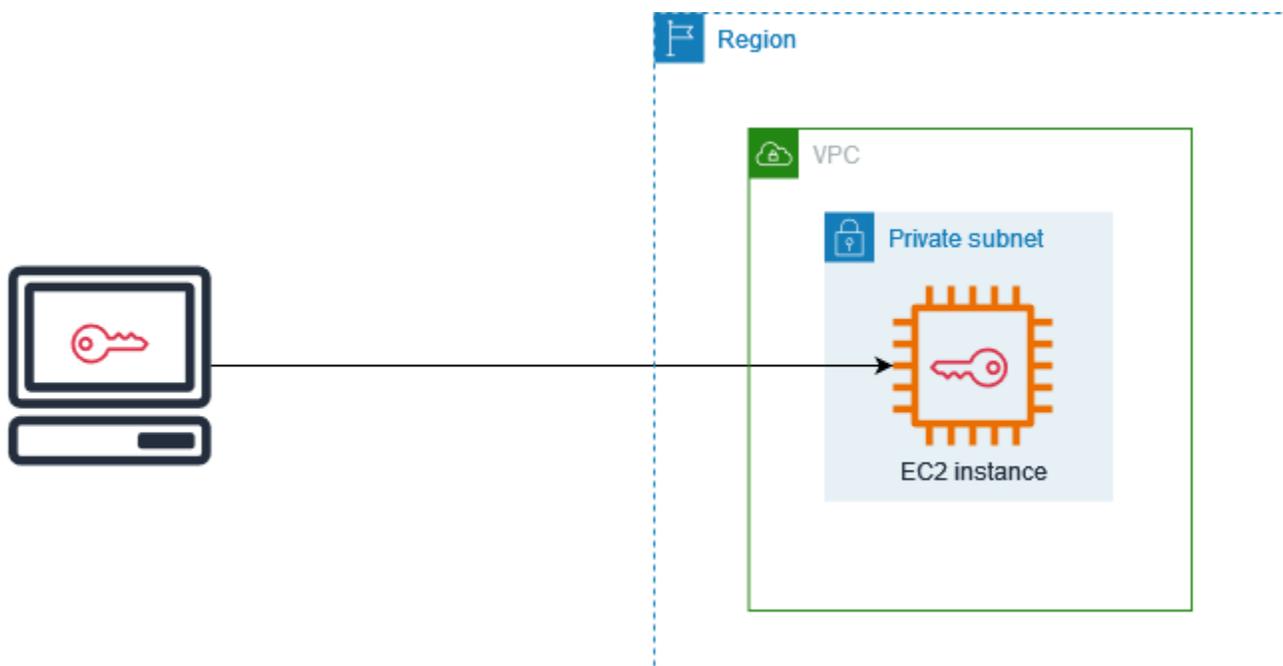
AWS CloudTrail AWS Config, et AWS Config Rules fournissent des fonctionnalités d'audit et de suivi des modifications pour auditer les modifications AWS des ressources. Configurez les journaux d'événements Windows pour envoyer des fichiers journaux locaux à un système de gestion centralisée des journaux, afin de préserver les données des journaux à des fins d'analyse de la sécurité et du comportement opérationnel. Microsoft System Center Operations Manager (SCOM) regroupe les informations concernant les applications Microsoft déployées sur des instances Windows et applique des jeux de règles préconfigurés et personnalisés basés sur les rôles et services d'application. System Center Management Packs s'appuie sur SCOM pour fournir des conseils de configuration et de surveillance spécifiques aux applications. Ces [packs d'administration](#) prennent en charge Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014 et de nombreux autres serveurs et technologies.

Outre les outils de gestion des systèmes Microsoft, les clients peuvent utiliser Amazon CloudWatch pour surveiller l'utilisation du processeur des instances, les performances du disque, les E/S réseau et effectuer des vérifications de l'état de l'hôte et de l'instance. Les agents de lancement EC2Config, EC2Launch et EC2Launch v2 donnent accès à des fonctionnalités avancées supplémentaires pour les instances Windows. Par exemple, ils peuvent exporter les journaux du système Windows, de la sécurité, des applications et des services Internet (IIS) vers CloudWatch des journaux qui peuvent ensuite être intégrés aux CloudWatch métriques et aux alarmes Amazon. Les clients peuvent également créer des scripts qui exportent les compteurs de performance Windows vers des métriques CloudWatch personnalisées Amazon.

Paires de clés Amazon EC2 et instances Amazon EC2

Une paire de clés, composée d'une clé privée et d'une clé publique, est un ensemble d'information d'identification que vous utilisez pour prouver votre identité lors de la connexion à une instance Amazon EC2. Pour les instances Linux, la clé privée vous permet d'accéder à votre instance par SSH en toute sécurité. Pour les instances Windows, la clé privée est requise pour déchiffrer le mot de passe administrateur, que vous utilisez ensuite pour vous connecter à votre instance.

Amazon EC2 stocke la clé publique sur votre instance, et vous stockez la clé privée, comme indiqué dans le schéma suivant. Il est important de stocker votre clé privée dans un endroit sécurisé, car toute personne possédant votre clé privée peut se connecter à vos instances qui utilisent la paire de clés.



Lorsque vous lancez une instance, vous pouvez [spécifier une paire de clés](#) afin de pouvoir vous connecter à votre instance à l'aide d'une méthode qui nécessite une paire de clés. Selon la façon dont vous gérez votre sécurité, vous pouvez spécifier la même paire de clés pour toutes vos instances ou vous pouvez spécifier différentes paires de clés.

Pour les instances Linux, lorsque votre instance démarre pour la première fois, la clé publique que vous avez spécifiée au lancement est placée sur votre instance Linux dans une entrée située à l'intérieur `~/.ssh/authorized_keys`. Lorsque vous vous connectez à votre instance Linux en utilisant le protocole SSH, vous devez spécifier la clé privée correspondant à la clé publique.

Pour plus d'informations sur la connexion à votre instance EC2, consultez [Connectez-vous à votre instance EC2](#).

Important

Dans la mesure où Amazon EC2 ne conserve pas de copie de votre clé privée, si vous la perdez, il n'est pas possible de la récupérer. Cependant, il peut toujours y avoir un moyen de vous connecter aux instances pour lesquelles vous avez perdu la clé privée. Pour plus d'informations, consultez [J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Linux ?](#).

Comme alternative aux paires de clés, vous pouvez vous connecter [AWS Systems Manager Session Manager](#) à votre instance à l'aide d'un shell interactif basé sur un navigateur en un clic ou du AWS Command Line Interface (CLI).

Table des matières

- [Créez une paire de clés pour votre instance Amazon EC2](#)
- [Baliser une paire de clés](#)
- [Décrivez vos paires de clés](#)
- [Supprimer votre paire de clés](#)
- [Ajouter ou supprimer une clé publique sur votre instance Linux](#)
- [Vérifier l'empreinte de votre paire de clés](#)

Créez une paire de clés pour votre instance Amazon EC2

Vous pouvez utiliser Amazon EC2 pour créer vos paires de clés, ou vous pouvez utiliser un outil tiers pour créer vos paires de clés, puis les importer dans Amazon EC2.

Amazon EC2 prend en charge les clés RSA SSH-2 2048 bits pour les instances Linux et Windows. Amazon EC2 prend également en charge les clés ED25519 pour les instances Linux.

Pour savoir comment vous connecter à votre instance Linux à l'aide de SSH après avoir créé une paire de clés, consultez [the section called “Connectez-vous à votre instance Linux”](#).

Pour savoir comment vous connecter à votre instance Windows à l'aide du protocole RDP après avoir créé une paire de clés, consultez [the section called “Connexion à votre instance Windows”](#).

Table des matières

- [Créer une paire de clés à l'aide d'Amazon EC2](#)
- [Créez une paire de clés en utilisant AWS CloudFormation](#)
- [Créer une paire de clés à l'aide d'un outil tiers et importer la clé publique dans Amazon EC2](#)

Créer une paire de clés à l'aide d'Amazon EC2

Lorsque vous créez une paire de clés à l'aide d'Amazon EC2, la clé publique est stockée dans Amazon EC2 et c'est vous qui stockez la clé privée.

Vous pouvez créer jusqu'à 5 000 paires de clés par région. Pour demander une augmentation, créez un dossier de support. Pour obtenir plus d'informations, consultez la section [Creating a support case](#) (Création d'un cas de support) dans le Guide de l'utilisateur AWS Support .

Console

Pour créer une paire de clés à l'aide d'Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Network & Security, choisissez Key Pairs.
3. Choisissez Créer une paire de clés.
4. Pour Name (Nom), entrez un nom descriptif pour la paire de clés. Amazon EC2 associe la clé publique au nom de clé que vous spécifiez. Le nom peut inclure jusqu'à 255 caractères ASCII. Il ne peut pas inclure d'espaces de début ou de fin.

- Sélectionnez un type de paire de clés adapté à votre système d'exploitation :

(Instances Linux) Pour le type de paire de clés, choisissez RSA ou ED25519.

(Instances Windows) Pour le type de paire de clés, choisissez RSA. Les clés ED25519 ne sont pas prises en charge pour les instances Windows.

- Pour le Private Key File format (Format de fichier de clé privée), sélectionnez le format dans lequel vous souhaitez enregistrer la clé privée. Pour enregistrer la clé privée dans un format qui peut être utilisé avec OpenSSH, choisissez pem. Pour enregistrer la clé privée dans un format qui peut être utilisé avec PuTTY, choisissez ppk.
- Pour ajouter une balise à la clé publique, sélectionnez Add tag (Ajouter une balise), puis entrez la clé et la valeur de la balise. Répétez l'opération pour chaque étiquette.
- Choisissez Créer une paire de clés.
- Le fichier de clé privée est automatiquement téléchargé dans votre navigateur. Le nom de fichier de base est celui que vous avez spécifié pour votre paire de clés, et l'extension de nom de fichier est déterminée par le format de fichier que vous avez choisi. Enregistrez le fichier de clé privée en lieu sûr.

 Important

C'est votre seule occasion d'enregistrer le fichier de clé privée.

- (Instances Linux) Si vous envisagez d'utiliser un client SSH sur un ordinateur macOS ou Linux pour vous connecter à votre instance Linux, utilisez la commande suivante pour définir les autorisations de votre fichier de clé privée afin que vous soyez le seul à pouvoir le lire.

```
chmod 400 key-pair-name.pem
```

Si vous ne définissez pas ces autorisations, vous ne pouvez pas vous connecter à votre instance à l'aide de cette paire de clés. Pour plus d'informations, consultez [Erreur : fichier de clé privée non protégé](#).

AWS CLI

Pour créer une paire de clés à l'aide d'Amazon EC2

1. Pour générer la paire de clés et enregistrer la clé privée vers un fichier `.pem`, utilisez la commande [create-key-pair](#) comme suit.

Pour `--key-name`, indiquez un nom pour la clé publique. Le nom peut inclure jusqu'à 255 caractères ASCII.

Pour `--key-type`, spécifiez `rsa` ou `ed25519`. Si vous n'incluez pas le paramètre `--key-type`, une clé `rsa` est créée par défaut. Notez que les clés ED25519 ne sont pas prises en charge pour les instances Windows.

Pour `--key-format`, spécifiez `pem` ou `ppk`. Si vous n'incluez pas le paramètre `--key-format`, un fichier `pem` est créé par défaut.

`--query "KeyMaterial"` imprime le matériel de clé privée à la sortie.

`--output text > my-key-pair.pem` enregistre le matériel de clé privée dans un fichier avec l'extension spécifiée. L'extension peut être `.pem` ou `.ppk`. La clé privée peut avoir un nom différent de la clé publique, mais pour faciliter son utilisation, utilisez le même nom.

```
aws ec2 create-key-pair \  
  --key-name my-key-pair \  
  --key-type rsa \  
  --key-format pem \  
  --query "KeyMaterial" \  
  --output text > my-key-pair.pem
```

2. (Instances Linux) Si vous envisagez d'utiliser un client SSH sur un ordinateur macOS ou Linux pour vous connecter à votre instance Linux, utilisez la commande suivante pour définir les autorisations de votre fichier de clé privée afin que vous soyez le seul à pouvoir le lire.

```
chmod 400 key-pair-name.pem
```

Si vous ne définissez pas ces autorisations, vous ne pouvez pas vous connecter à votre instance à l'aide de cette paire de clés. Pour plus d'informations, consultez [Erreur : fichier de clé privée non protégé](#).

PowerShell

Pour créer une paire de clés à l'aide d'Amazon EC2

Utilisez la [New-EC2KeyPair](#) AWS Tools for Windows PowerShell commande suivante pour générer la clé et l'enregistrer dans un `.ppk` fichier `.pem` or.

Pour `-KeyName`, indiquez un nom pour la clé publique. Le nom peut inclure jusqu'à 255 caractères ASCII.

Pour `-KeyType`, spécifiez `rsa` ou `ed25519`. Si vous n'incluez pas le paramètre `-KeyType`, une clé `rsa` est créée par défaut. Notez que les clés ED25519 ne sont pas prises en charge pour les instances Windows.

Pour `-KeyFormat`, spécifiez `pem` ou `ppk`. Si vous n'incluez pas le paramètre `-KeyFormat`, un fichier `pem` est créé par défaut.

`KeyMaterial` imprime le matériel de clé privée à la sortie.

`Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem` enregistre le matériel de clé privée dans un fichier avec l'extension spécifiée. L'extension peut être `.pem` ou `.ppk`. La clé privée peut avoir un nom différent de la clé publique, mais pour faciliter son utilisation, utilisez le même nom.

```
PS C:\> (New-EC2KeyPair -KeyName "my-key-pair" -KeyType "rsa" -KeyFormat "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Créez une paire de clés en utilisant AWS CloudFormation

Lorsque vous créez une nouvelle paire de clés à l'aide de AWS CloudFormation, la clé privée est enregistrée dans AWS Systems Manager Parameter Store. Le nom du paramètre a le format suivant :

```
/ec2/keypair/key_pair_id
```

Pour plus d'informations, veuillez consulter la rubrique [AWS Systems Manager Parameter Store](#) dans le Guide de l'utilisateur AWS Systems Manager .

Pour créer une paire de clés en utilisant AWS CloudFormation

1. Spécifiez la [AWS::EC2::KeyPair](#) ressource dans votre modèle.

```
Resources:
  NewKeyPair:
    Type: 'AWS::EC2::KeyPair'
    Properties:
      KeyName: new-key-pair
```

- Utilisez la commande [describe-key-pairs](#) comme suit pour obtenir l'ID de la paire de clés.

```
aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
KeyPairs[*].KeyId --output text
```

Voici un exemple de sortie.

```
key-05abb699beEXAMPLE
```

- Utilisez la commande [get-parameter](#) comme suit pour obtenir le paramètre de votre clé et enregistrer le contenu de la clé dans un fichier `.pem`.

```
aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
--query Parameter.Value --output text > new-key-pair.pem
```

Autorisations IAM requises

AWS CloudFormation Pour permettre de gérer les paramètres du magasin de paramètres en votre nom, le rôle IAM assumé par AWS CloudFormation ou votre utilisateur doit disposer des autorisations suivantes :

- `ssm:PutParameter` : accorde l'autorisation de créer un paramètre pour le matériel de clé privée.
- `ssm:DeleteParameter` : autorise la suppression du paramètre utilisé pour stocker les éléments de clé privée. Cette autorisation est nécessaire, que la paire de clés ait été importée ou créée par AWS CloudFormation.

Lorsqu'il AWS CloudFormation supprime une paire de clés créée ou importée par une pile, il effectue une vérification des autorisations pour déterminer si vous êtes autorisé à supprimer des paramètres, même s'il AWS CloudFormation crée un paramètre uniquement lorsqu'il crée une paire de clés, et non lorsqu'il importe une paire de clés. AWS CloudFormation teste l'autorisation requise à l'aide d'un nom de paramètre fabriqué qui ne correspond à aucun paramètre de votre

compte. Par conséquent, vous pouvez voir un nom de paramètre fabriqué dans le message d'erreur `AccessDeniedException`.

Créer une paire de clés à l'aide d'un outil tiers et importer la clé publique dans Amazon EC2

Instances Linux

Vous pouvez créer une paire de clés RSA ou ED25519 à l'aide d'un outil tiers, puis importer la clé publique dans Amazon EC2, au lieu d'utiliser Amazon EC2 pour créer une paire de clés.

Exigences relatives aux paires de clés

- Types pris en charge : RSA et ED25519. Amazon EC2 n'accepte pas les clés DSA.
- Formats pris en charge :
 - Format de clé publique OpenSSH (format dans). `~/.ssh/authorized_keys` Si vous vous connectez avec SSH lorsque vous utilisez l'API EC2 Instance Connect, le format SSH2 est également pris en charge.
 - Le fichier de clé privée SSH doit être au format PEM ou PPK
 - Le format DER codé en base64 (RSA uniquement)
 - Le format de fichier de clé publique SSH tel que spécifié dans [RFC 4716](#) (RSA uniquement)
- Longueurs prises en charge : 1024, 2048 et 4096. Si vous vous connectez avec SSH lorsque vous utilisez l'API EC2 Instance Connect, les longueurs prises en charge sont 2 048 et 4096.

Pour créer une paire de clés à l'aide d'un outil tiers

1. Générez une paire de clés avec un outil tiers de votre choix. Par exemple, vous pouvez utiliser `ssh-keygen` (outil fourni avec l'installation OpenSSH standard). Java, Ruby, Python, ainsi qu'un grand nombre d'autres langages de programmation fournissent également des bibliothèques standard pouvant être utilisées pour créer une paire de clés RSA ou ED25519.

Important

La clé privée doit être au format PEM ou PPK. Par exemple, utilisez `ssh-keygen -m PEM` pour générer la clé OpenSSH au format PEM.

2. Enregistrez la clé publique dans un fichier local. Par exemple, `~/.ssh/my-key-pair.pub`. L'extension du nom de fichier de ce fichier n'est pas importante.

3. Enregistrez la clé privée dans un fichier local dont l'extension est `.pem` ou `.ppk`. Par exemple, `~/.ssh/my-key-pair.pem` ou `~/.ssh/my-key-pair.ppk`.

Important

Enregistrez le fichier de clé privée en lieu sûr. Vous devez fournir le nom de votre clé publique lorsque vous lancez une instance, ainsi que la clé privée correspondante chaque fois que vous vous connectez à l'instance.

instances Windows

Vous pouvez créer une paire de clés RSA à l'aide d'un outil tiers, puis importer la clé publique dans Amazon EC2, au lieu d'utiliser Amazon EC2 pour créer votre paire de clés.

Exigences relatives aux paires de clés

- Types pris en charge : RSA. Amazon EC2 n'accepte pas les clés DSA.

Note

Les clés ED25519 ne sont pas prises en charge pour les instances Windows.

- Formats pris en charge :
 - Format de clé publique OpenSSH
 - Le fichier de clé privée SSH doit être au format PEM ou PPK
 - Le format DER codé en base64 (RSA uniquement)
 - Le format de fichier de clé publique SSH tel que spécifié dans [RFC 4716](#) (RSA uniquement)
- Longueurs prises en charge : 1024, 2048 et 4096.

Pour créer une paire de clés à l'aide d'un outil tiers

1. Générez une paire de clés avec un outil tiers de votre choix. Par exemple, vous pouvez utiliser `ssh-keygen` (outil fourni avec l'installation OpenSSH standard). Java, Ruby, Python, ainsi qu'un grand nombre d'autres langages de programmation fournissent également des bibliothèques standard pouvant être utilisées pour créer une paire de clés RSA.

⚠ Important

La clé privée doit être au format PEM ou PPK. Par exemple, utilisez `ssh-keygen -m PEM` pour générer la clé OpenSSH au format PEM.

2. Enregistrez la clé publique dans un fichier local. Par exemple, `C:\keys\my-key-pair.pub`. L'extension du nom de fichier de ce fichier n'est pas importante.
3. Enregistrez la clé privée dans un fichier local dont l'extension est `.pem` ou `.ppk`. Par exemple, `C:\keys\my-key-pair.pem` ou `C:\keys\my-key-pair.ppk`. L'extension du nom de fichier de ce fichier est importante car seuls `.pem` les fichiers peuvent être sélectionnés lors de la connexion à votre instance Windows depuis la console EC2.

⚠ Important

Enregistrez le fichier de clé privée en lieu sûr. Vous devez fournir le nom de votre clé publique lorsque vous lancez une instance, ainsi que la clé privée correspondante chaque fois que vous vous connectez à l'instance.

Après avoir créé la paire de clés, utilisez l'une des méthodes suivantes pour importer votre clé publique vers Amazon EC2.

Console

Pour importer la clé publique dans Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, cliquez sur Key Pairs.
3. Choisissez Import key pair (Importer une paire de clés).
4. Pour Name (Nom), saisissez un nom descriptif pour la clé publique. Le nom peut inclure jusqu'à 255 caractères ASCII. Il ne peut pas inclure d'espaces de début ou de fin.

📘 Note

Lorsque vous vous connectez à votre instance à partir de la console EC2, la console suggère ce nom pour le nom de votre fichier de clé privée.

5. Choisissez Browse (Parcourir) pour accéder à votre clé publique et la sélectionner, ou collez le contenu de votre clé publique dans le champ Public key contents (Contenu de la clé publique).
6. Choisissez Import key pair (Importer une paire de clés).
7. Vérifiez que la clé publique que vous avez importée apparaît dans la liste des paires de clés.

AWS CLI

Pour importer la clé publique dans Amazon EC2

Utilisez la commande [import-key-pair](#) AWS CLI .

Pour vérifier que la paire de clés a été importée correctement

Utilisez la commande [describe-key-pairs](#) AWS CLI .

PowerShell

Pour importer la clé publique dans Amazon EC2

Utilisez la commande [Import-EC2KeyPair](#) AWS Tools for Windows PowerShell .

Pour vérifier que la paire de clés a été importée correctement

Utilisez la commande [Get-EC2KeyPair](#) AWS Tools for Windows PowerShell .

Baliser une paire de clés

Pour classer et gérer les paires de clés que vous avez créées à l'aide d'Amazon EC2 ou importées dans Amazon EC2, vous pouvez les baliser avec des métadonnées personnalisées. Pour plus d'informations sur le fonctionnement des balises, consultez [Baliser vos ressources Amazon EC2](#).

Console

Pour afficher, ajouter ou supprimer le tag d'une paire de clés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, cliquez sur Key Pairs.
3. Sélectionnez une clé publique, puis choisissez Actions, Gérer les étiquettes.
4. La page Gérer les étiquettes) affiche toutes les étiquettes affectées à la clé publique.

- Pour ajouter une balise, choisissez Ajouter la balise, puis entrez la clé et la valeur de la balise. Vous pouvez ajouter jusqu'à 50 étiquettes par clé. Pour plus d'informations, consultez [Restrictions liées aux balises](#).
- Pour supprimer une balise, sélectionnez Remove (Retirer) en regard de la zone de valeur de la balise.

5. Choisissez Enregistrer.

AWS CLI

Pour afficher les tags de vos paires de clés

Utilisez la commande [describe-tags](#) AWS CLI . Dans l'exemple suivant, vous décrivez les étiquettes de toutes vos clés publiques.

```
aws ec2 describe-tags --filters "Name=resource-type,Values=key-pair"
```

```
{
  "Tags": [
    {
      "Key": "Environment",
      "ResourceId": "key-0123456789EXAMPLE",
      "ResourceType": "key-pair",
      "Value": "Production"
    },
    {
      "Key": "Environment",
      "ResourceId": "key-9876543210EXAMPLE",
      "ResourceType": "key-pair",
      "Value": "Production"
    }
  ]
}
```

Pour décrire les balises d'une paire de clés

Utilisez la commande [describe-key-pairs](#) AWS CLI .

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789EXAMPLE
```

```
{
```

```
"KeyPairs": [  
  {  
    "KeyName": "MyKeyPair",  
    "KeyFingerprint":  
    "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",  
    "KeyPairId": "key-0123456789EXAMPLE",  
    "Tags": [  
      {  
        "Key": "Environment",  
        "Value": "Production"  
      }  
    ]  
  }  
]
```

Pour étiqueter une paire de clés

Utilisez la commande [create-tags](#) AWS CLI . Dans l'exemple suivant, la clé publique est étiquetée avec `Key=Cost-Center` et `Value=CC-123`.

```
aws ec2 create-tags --resources key-0123456789EXAMPLE --tags Key=Cost-Center,Value=CC-123
```

Pour supprimer une balise d'une paire de clés

Utilisez la commande [delete-tags](#) AWS CLI . Pour obtenir des exemples, reportez-vous à la section [Exemples](#) dans le document AWS CLI Références des commandes.

PowerShell

Pour afficher les tags de vos paires de clés

Utilisez la commande [Get-EC2Tag](#).

Pour décrire les balises d'une paire de clés

Utilisez la commande [Get-EC2KeyPair](#).

Pour étiqueter une paire de clés

Utilisez la commande [New-EC2Tag](#).

Pour supprimer une balise d'une paire de clés

Utilisez la commande [Remove-EC2Tag](#).

Décrivez vos paires de clés

Vous pouvez décrire les paires de clés que vous avez stockées dans Amazon EC2. Vous pouvez également récupérer le contenu de la clé publique et identifier la clé publique spécifiée lors du lancement.

Rubriques

- [Décrivez vos paires de clés](#)
- [Extraire le contenu de la clé publique](#)
- [Identifier la clé publique spécifiée au lancement](#)

Décrivez vos paires de clés

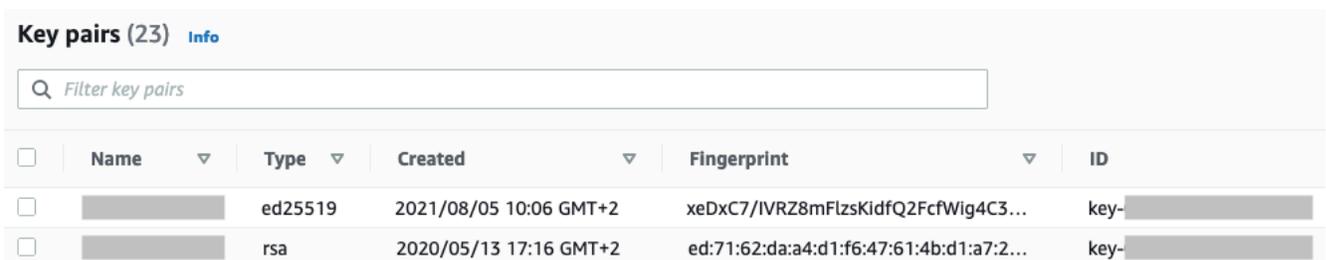
Vous pouvez afficher les informations suivantes sur vos clés publiques stockées dans Amazon EC2 : nom de la clé publique, ID, type de clé, empreinte digitale, matériel de clé publique, date et heure (fuseau horaire UTC) à laquelle la clé a été créée par Amazon EC2 (si la clé a été créée par un outil tiers, il s'agit de la date et de l'heure auxquelles la clé a été importée dans Amazon EC2), ainsi que toutes les identifications associées à la clé publique.

Vous pouvez utiliser la console Amazon EC2 ou consulter les informations relatives AWS CLI à vos clés publiques.

Console

Pour afficher des informations sur vos clés publiques

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, choisissez Key Pairs (Paires de clés).
3. Vous pouvez afficher les informations relatives à chaque clé publique dans la table Key pairs (Paires de clés).



<input type="checkbox"/>	Name	Type	Created	Fingerprint	ID
<input type="checkbox"/>		ed25519	2021/08/05 10:06 GMT+2	xeDxC7/IVRZ8mFlzsKidfQ2FcfWig4C3...	key-
<input type="checkbox"/>		rsa	2020/05/13 17:16 GMT+2	ed:71:62:da:a4:d1:f6:47:61:4b:d1:a7:2...	key-

4. Pour afficher les identifications d'une clé publique, cochez la case à côté de la clé, puis choisissez Actions, Manage tags (Gérer les identifications).

AWS CLI

Pour décrire une clé publique

Utilisez la commande [describe-key-pairs](#) et spécifiez le paramètre `--key-names`.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

Exemple de sortie

```
{
  "KeyPairs": [
    {
      "KeyPairId": "key-0123456789example",
      "KeyFingerprint":
"1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
      "KeyName": "key-pair-name",
      "KeyType": "rsa",
      "Tags": [],
      "CreateTime": "2022-04-28T11:37:26.000Z"
    }
  ]
}
```

Sinon, au lieu de `--key-names`, vous pouvez spécifier le paramètre `--key-pair-ids` pour identifier la clé publique.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example
```

Pour afficher la clé publique dans la sortie, vous devez spécifier le paramètre `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Exemple de sortie : dans la sortie, le champ `PublicKey` contient la clé publique.

```
{
```

```
"KeyPairs": [  
  {  
    "KeyPairId": "key-0123456789example",  
    "KeyFingerprint":  
"1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",  
    "KeyName": "key-pair-name",  
    "KeyType": "rsa",  
    "Tags": [],  
    "PublicKey": "ssh-ed25519  
AAAAC3NzaC1lZDI1NTE5AAAAIij7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",  
    "CreateTime": "2022-04-28T11:37:26.000Z"  
  }  
]  
}
```

Extraire le contenu de la clé publique

Vous pouvez utiliser différentes méthodes pour accéder à la clé publique. Vous pouvez récupérer le contenu de la clé publique à partir de la clé privée correspondante sur votre ordinateur local, à partir des métadonnées de l'instance lancée avec la clé publique ou à l'aide de la `describe-key-pairs` AWS CLI commande. Pour les instances Linux, le contenu de la clé publique peut également être extrait du `authorized_keys` fichier de l'instance.

Utilisez l'une des méthodes suivantes pour récupérer le contenu de la clé publique.

Instances Linux

From the private key

Pour extraire le contenu de la clé publique de la clé privée

Sur votre ordinateur local Linux ou macOS, vous pouvez utiliser la commande `ssh-keygen` pour extraire la clé publique de votre paire de clés. Spécifiez le chemin où vous avez téléchargé votre clé privée (fichier `.pem`).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

La commande renvoie la clé publique, comme indiqué dans l'exemple suivant.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCLKsfbkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzo0WbkM4yxyb/wB96xbiFveSFJu0p/d6RJhJ0I0iBXr
```

```
lsLnBItnctkiJ7FbtXJMXLvwwJryDUi1BMTjYtwB+QhYXUM0zce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb  
BQoQzd8v7yeb70z1Pnw0yN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Si la commande échoue, exécutez la commande suivante pour vous assurer d'avoir modifié les autorisations sur votre fichier de paire de clés privées afin d'être le seul à pouvoir l'afficher.

```
chmod 400 key-pair-name.pem
```

From the instance metadata

Vous pouvez utiliser le service des métadonnées d'instance Version 2 ou le service des métadonnées d'instance Version 1 pour récupérer la clé publique à partir des métadonnées de l'instance.

Note

Si vous modifiez la paire de clés que vous utilisez pour vous connecter à l'instance, Amazon EC2 ne met pas à jour les métadonnées de l'instance pour afficher la nouvelle clé publique. Les métadonnées d'instance continuent d'afficher la clé publique pour la paire de clés que vous avez spécifiée lors du lancement de l'instance.

Pour récupérer le contenu de la clé publique à partir des métadonnées de l'instance

Utilisez l'une des commandes suivantes pour vous connecter à votre instance.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-  
aws-ec2-metadata-token-ttl-seconds: 21600" ` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-  
data/public-keys/0/openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Exemple de sortie

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzo0WbkM4yxyb/wB96xbiFveSFJu0p/d6RJhJ0I0iBXr
lsLnBItnctkiJ7FbtXJMXLvvwJryDUi1BMTjYtwB+QhYXUM0zce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WriUBkrHmFJr6HcXkvJdWPKYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb70z1PnW0yN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Pour obtenir plus d'informations sur les métadonnées d'instance, consultez [Récupérer des métadonnées d'instance](#).

From the instance

Si vous spécifiez une paire de clés lorsque vous lancez une instance Linux, lorsque l'instance démarre pour la première fois, le contenu de la clé publique est placé sur l'instance dans une entrée dans `~/.ssh/authorized_keys`.

Pour récupérer le contenu de la clé publique à partir d'une instance

1. [Connectez-vous à votre instance](#).
2. Dans la fenêtre du terminal, ouvrez le fichier `authorized_keys` à l'aide de votre éditeur de texte préféré (tel que `vim` ou `nano`).

```
[ec2-user ~]$ nano ~/.ssh/authorized_keys
```

Le fichier `authorized_keys` s'ouvre, affichant la clé publique, suivie du nom de la paire de clés. Voici un exemple d'entrée pour la paire de clés nommée *key-pair-name*.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzo0WbkM4yxyb/wB96xbiFveSFJu0p/d6RJhJ0I0iBXr
lsLnBItnctkiJ7FbtXJMXLvvwJryDUi1BMTjYtwB+QhYXUM0zce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WriUBkrHmFJr6HcXkvJdWPKYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb70z1PnW0yN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

From describe-key-pairs

Pour extraire la clé publique à partir de la commande `AWS CLI describe-key-pairs`

Utilisez la commande [describe-key-pairs](#) et spécifiez le paramètre `--key-names` pour identifier la clé publique. Pour inclure la clé publique dans la sortie, spécifiez le paramètre `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Exemple de sortie : dans la sortie, le champ `PublicKey` contient la clé publique.

```
{
  "KeyPairs": [
    {
      "KeyPairId": "key-0123456789example",
      "KeyFingerprint":
"1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
      "KeyName": "key-pair-name",
      "KeyType": "rsa",
      "Tags": [],
      "PublicKey": "ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIIj7az1DjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
      "CreateTime": "2022-04-28T11:37:26.000Z"
    }
  ]
}
```

Sinon, au lieu de `--key-names`, vous pouvez spécifier le paramètre `--key-pair-ids` pour identifier la clé publique.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

instances Windows

From the private key

Pour extraire le contenu de la clé publique de la clé privée

Sur votre ordinateur Windows local, vous pouvez utiliser PuTTYgen pour obtenir la clé publique de votre paire de clés.

Lancez PuTTYgen et choisissez Load (Charger). Sélectionnez le fichier de clé privée `.ppk` ou `.pem`. PuTTYgen affiche la clé publique sous Public key for pasting into OpenSSH authorized_keys file (Clé publique à coller dans le fichier `authorized_keys` OpenSSH). Vous pouvez également visualiser la clé publique en choisissant Save public key (Enregistrer la clé publique), en spécifiant un nom pour le fichier, en enregistrant le fichier et en ouvrant le fichier.

From the instance metadata

Vous pouvez utiliser le service des métadonnées d'instance Version 2 ou le service des métadonnées d'instance Version 1 pour récupérer la clé publique à partir des métadonnées de l'instance.

Note

Si vous modifiez la paire de clés que vous utilisez pour vous connecter à l'instance, Amazon EC2 ne met pas à jour les métadonnées de l'instance pour afficher la nouvelle clé publique. Les métadonnées d'instance continuent d'afficher la clé publique pour la paire de clés que vous avez spécifiée lors du lancement de l'instance.

Pour récupérer le contenu de la clé publique à partir des métadonnées de l'instance

Utilisez l'une des commandes suivantes pour vous connecter à votre instance.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Exemple de sortie

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706Vhz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzo0WbkM4yxyb/wB96xbiFveSFJu0p/d6RJhJ0I0iBXrlsLnBItnctkiJ7FbtXJMXLvwwJryDUilBMTjYtwB+QhYXUM0zce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3RbBQoQzd8v7yeb70z1Pnw0yN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Pour obtenir plus d'informations sur les métadonnées d'instance, consultez [Récupérer des métadonnées d'instance](#).

From describe-key-pairs

Pour extraire la clé publique à partir de la commande AWS CLI **describe-key-pairs**

Utilisez la commande [describe-key-pairs](#) et spécifiez le paramètre `--key-names` pour identifier la clé publique. Pour inclure la clé publique dans la sortie, spécifiez le paramètre `--include-public-key`.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Exemple de sortie : dans la sortie, le champ `PublicKey` contient la clé publique.

```
{
  "KeyPairs": [
    {
      "KeyPairId": "key-0123456789example",
      "KeyFingerprint":
"1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
      "KeyName": "key-pair-name",
      "KeyType": "rsa",
      "Tags": [],
      "PublicKey": "ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIIj7az1DjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
      "CreateTime": "2022-04-28T11:37:26.000Z"
    }
  ]
}
```

Sinon, au lieu de `--key-names`, vous pouvez spécifier le paramètre `--key-pair-ids` pour identifier la clé publique.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

Identifier la clé publique spécifiée au lancement

Si vous spécifiez une clé publique lorsque vous lancez une instance, le nom de la clé publique est enregistré par l'instance.

Pour identifier la clé publique spécifiée au lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Sous l'onglet Détails, sous Détails de l'instance, le champ Paire de clés assignée au lancement affiche le nom de la clé publique que vous avez spécifiée lors du lancement de l'instance.

Note

La valeur du champ Paire de clés assignée au lancement ne change pas même si vous modifiez la clé publique sur l'instance ou si vous ajoutez des clés publiques.

Supprimer votre paire de clés

Vous pouvez supprimer une paire de clés, ce qui supprime la clé publique stockée dans Amazon EC2. La suppression d'une paire de clés ne supprime pas la clé privée correspondante.

Lorsque vous supprimez une clé publique à l'aide des méthodes suivantes, vous supprimez uniquement la clé publique que vous avez enregistrée dans Amazon EC2 lorsque vous avez [créé](#) ou [importé](#) la paire de clés. La suppression d'une clé publique ne supprime pas la clé publique des instances auxquelles vous l'avez ajoutée, que vous l'ayez ajoutée lors du lancement de l'instance ou plus tard. Elle ne supprime pas non plus la clé privée présente sur votre ordinateur local. Vous pouvez continuer à vous connecter aux instances que vous avez lancées à l'aide d'une clé publique que vous avez supprimée d'Amazon EC2, tant que vous disposez de la clé privée (fichier .pem).

Important

Si vous utilisez un groupe Auto Scaling (par exemple, dans un environnement Elastic Beanstalk), assurez-vous que la clé publique que vous supprimez n'est pas spécifiée dans un modèle de lancement ou dans une configuration de lancement associé(e). Si Amazon EC2 Auto Scaling détecte une instance défectueuse, il lance une instance de remplacement. Toutefois, le lancement de l'instance échoue si la clé publique est introuvable. Pour plus d'informations, consultez [Modèles de lancement](#) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

Console

Pour supprimer votre clé publique sur Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, cliquez sur Key Pairs.
3. Sélectionnez la paire de clés à supprimer et choisissez Actions, Delete (Supprimer).
4. Dans le champ de confirmation, entrez, DeLeTe puis choisissez Delete (Supprimer).

AWS CLI

Pour supprimer votre clé publique sur Amazon EC2

Utilisez la commande [delete-key-pair](#) AWS CLI .

PowerShell

Pour supprimer votre clé publique sur Amazon EC2

Utilisez la commande [Remove-EC2KeyPair](#) AWS Tools for Windows PowerShell .

Ajouter ou supprimer une clé publique sur votre instance Linux

Si vous perdez une clé privée, vous perdez l'accès à toutes les instances qui utilisent la paire de clés. Pour plus d'informations sur la connexion à une instance à l'aide d'une paire de clés différente de celle que vous avez spécifiée au lancement, voir [J'ai perdu ma clé privée](#).

Lorsque vous lancez une instance, vous pouvez [spécifier une paire de clés](#). Si vous spécifiez une paire de clés lors du lancement, lorsque votre instance démarre pour la première fois, le contenu de la clé publique est placé sur votre instance Linux dans une entrée dans `~/.ssh/authorized_keys`.

Vous pouvez modifier la paire de clés utilisée pour accéder au compte système par défaut de votre instance en ajoutant une nouvelle clé publique sur l'instance ou en remplaçant la clé publique (en supprimant la clé publique existante et en ajoutant une nouvelle clé) sur l'instance. Vous pouvez également supprimer toutes les clés publiques d'une instance. Pour ajouter ou remplacer une paire de clés, vous devez pouvoir vous connecter à votre instance.

Vous pouvez ajouter ou remplacer une paire de clés pour les raisons suivantes :

- Si un utilisateur de votre organisation requiert l'accès à l'utilisateur système à l'aide d'une paire de clés distincte, vous pouvez ajouter la clé publique à votre instance.
- Si quelqu'un possède une copie de la clé privée (fichier `.pem`) et que vous voulez l'empêcher de se connecter à votre instance (par exemple, si la personne a quitté votre organisation), vous pouvez supprimer la clé publique sur l'instance et la remplacer par une nouvelle.
- Si vous créez une AMI Linux à partir d'une instance, le contenu de la clé publique est copié de l'instance vers l'AMI. Si vous lancez une instance à partir de l'AMI, la nouvelle instance comprend la clé publique de l'instance d'origine. Pour empêcher une personne disposant de la clé privée de se connecter à la nouvelle instance, vous pouvez supprimer la clé publique de l'instance d'origine avant la création de l'AMI.

Utilisez les procédures suivantes pour modifier la paire de clés de l'utilisateur par défaut, par exemple `ec2-user`. Pour plus d'informations sur l'ajout d'utilisateurs à votre instance, consultez la documentation du système d'exploitation de votre instance.

Pour ajouter ou remplacer une paire de clés

1. Créez une nouvelle paire de clés à l'aide de [la console Amazon EC2](#) ou d'un [outil tiers](#).
2. Récupérez la clé publique de votre nouvelle paire de clés. Pour plus d'informations, consultez [Extraire le contenu de la clé publique](#).
3. [Connectez-vous à votre instance](#) à l'aide de votre clé privée existante.
4. À l'aide d'un éditeur de texte de votre choix, ouvrez le fichier `.ssh/authorized_keys` sur l'instance. Collez les informations de clé publique depuis votre nouvelle paire de clés sous les informations existantes de clé publique. Sauvegardez le fichier.
5. Déconnectez-vous de votre instance et testez que vous pouvez vous connecter à votre instance à l'aide du nouveau fichier de clé privé.
6. (Facultatif) Si vous remplacez une paire de clés existante, connectez-vous à votre instance et supprimez les informations de clé publique de la paire de clés originale du fichier `.ssh/authorized_keys`.

Important

Si vous utilisez un groupe Auto Scaling, assurez-vous que la paire de clés que vous remplacez n'est pas spécifiée dans votre modèle ou votre configuration de lancement. Si Amazon EC2 Auto Scaling détecte une instance défectueuse, il lance une instance de remplacement. Toutefois, le lancement de l'instance échoue si la paire de clés est introuvable. Pour plus d'informations, consultez [Modèles de lancement](#) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

Pour supprimer une clé publique d'une instance

1. [Connectez-vous à votre instance.](#)
2. À l'aide d'un éditeur de texte de votre choix, ouvrez le fichier `.ssh/authorized_keys` sur l'instance. Supprimez les informations de clé publique, puis enregistrez le fichier.

Warning

Après avoir supprimé toutes les clés publiques d'une instance et vous être déconnecté de l'instance, vous ne pouvez pas vous connecter à nouveau à moins que l'AMI ne fournisse une autre méthode de connexion.

Vérifier l'empreinte de votre paire de clés

Pour vérifier l'empreinte de votre paire de clés, comparez l'empreinte affichée sur la page Paires de clés de la console Amazon EC2 ou renvoyée par la commande [describe-key-pairs](#), à l'empreinte que vous générez à l'aide de la clé privée sur votre ordinateur local. Ces empreintes doivent correspondre.

Lorsque Amazon EC2 calcule une empreinte, Amazon EC2 peut ajouter un remplissage à l'empreinte avec des caractères `=`. D'autres outils, tels que `ssh-keygen`, pourraient omettre ce remplissage.

Si vous essayez de vérifier l'empreinte de votre instance Linux EC2, et non celle de votre paire de clés, consultez [Obtenir l'empreinte de l'instance.](#)

Comment sont calculées les empreintes

Amazon EC2 utilise différentes fonctions de hachage pour calculer les empreintes des paires de clés RSA et ED25519. En outre, pour les paires de clés RSA, Amazon EC2 calcule les empreintes différemment en utilisant différentes fonctions de hachage selon que la paire de clés a été créée par Amazon EC2 ou importée dans Amazon EC2.

Le tableau suivant répertorie les fonctions de hachage utilisées pour calculer les empreintes pour les paires de clés RSA et ED25519 qui sont créées par Amazon EC2 et importées dans Amazon EC2.

(Instances Linux) Fonctions de hachage utilisées pour calculer les empreintes

Source de paires de clés	Paires de clés RSA (Windows et Linux)	Paires de clés ED25519 (Linux)
Créées par Amazon EC2	SHA-1	SHA-256
Importées dans Amazon EC2	MD5 ¹	SHA-256

¹ Si vous importez une clé publique RSA dans Amazon EC2, l'empreinte est calculée à l'aide d'une fonction de hachage MD5. Ceci est vrai quelle que soit la manière dont vous avez créé la paire de clés, par exemple, en utilisant un outil tiers ou en générant une nouvelle clé publique à partir d'une clé privée existante créée à l'aide d'Amazon EC2.

Lorsque vous utilisez la même paire de clés dans différentes régions

Si vous prévoyez d'utiliser la même paire de clés pour vous connecter à des instances situées dans des instances différentes Régions AWS, vous devez importer la clé publique dans toutes les régions dans lesquelles vous l'utiliserez. Si vous utilisez Amazon EC2 pour créer la paire de clés, vous pouvez [Extraire le contenu de la clé publique](#) afin d'importer la clé publique dans les autres régions.

Note

- Si vous créez une paire de clés RSA à l'aide d'Amazon EC2 et que vous générez ensuite une clé publique à partir de la clé privée Amazon EC2, les clés publiques importées auront une empreinte digitale différente de celle de la clé publique d'origine. Cela est dû au fait que l'empreinte de la clé RSA originale créée à l'aide d'Amazon EC2 est calculée à l'aide d'une fonction de hachage SHA-1, tandis que l'empreinte digitale des clés RSA importées est calculée à l'aide d'une fonction de hachage MD5.

- Pour les paires de clés ED25519, les empreintes seront les mêmes, qu'elles soient créées par Amazon EC2 ou importées dans Amazon EC2, car la même fonction de hachage SHA-256 est utilisée pour calculer l'empreinte.

Générer une empreinte digitale à partir de la clé privée

Utilisez l'une des commandes suivantes pour générer une empreinte à partir de la clé privée sur votre machine locale.

Si vous utilisez une machine locale Windows, vous pouvez exécuter les commandes suivantes à l'aide de WSL (Windows Subsystem for Linux). Installez WSL et une distribution Linux à l'aide des instructions du [Guide d'installation de Windows 10](#). L'exemple des instructions installe la distribution Ubuntu de Linux, mais vous pouvez installer n'importe quelle distribution. Vous êtes invité à redémarrer votre ordinateur pour que les modifications prennent effet.

- Si vous avez créé la paire de clés à l'aide d'Amazon EC2

Utilisez les outils OpenSSL pour générer une empreinte comme indiqué dans les exemples suivants.

Pour les paires de clés RSA :

```
openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |  
openssl sha1 -c
```

(instances Linux) Pour les paires de clés ED25519 :

```
ssh-keygen -l -f path_to_private_key
```

- (Paires de clés RSA uniquement) Si vous avez importé la clé publique dans Amazon EC2

Vous pouvez suivre cette procédure quelle que soit la manière dont vous avez créé la paire de clés, par exemple, en utilisant un outil tiers ou en générant une nouvelle clé publique à partir d'une clé privée existante créée à l'aide d'Amazon EC2.

Utilisez les outils OpenSSL pour générer l'empreinte comme indiqué dans l'exemple suivant.

```
openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
```

- Si vous avez créé une paire de clés d'OpenSSH en utilisant OpenSSH 7.8 ou une version ultérieure et que vous avez importé la clé publique dans Amazon EC2

Utilisez `ssh-keygen` pour générer l'empreinte comme indiqué dans les exemples suivants.

Pour les paires de clés RSA :

```
ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER  
| openssl md5 -c
```

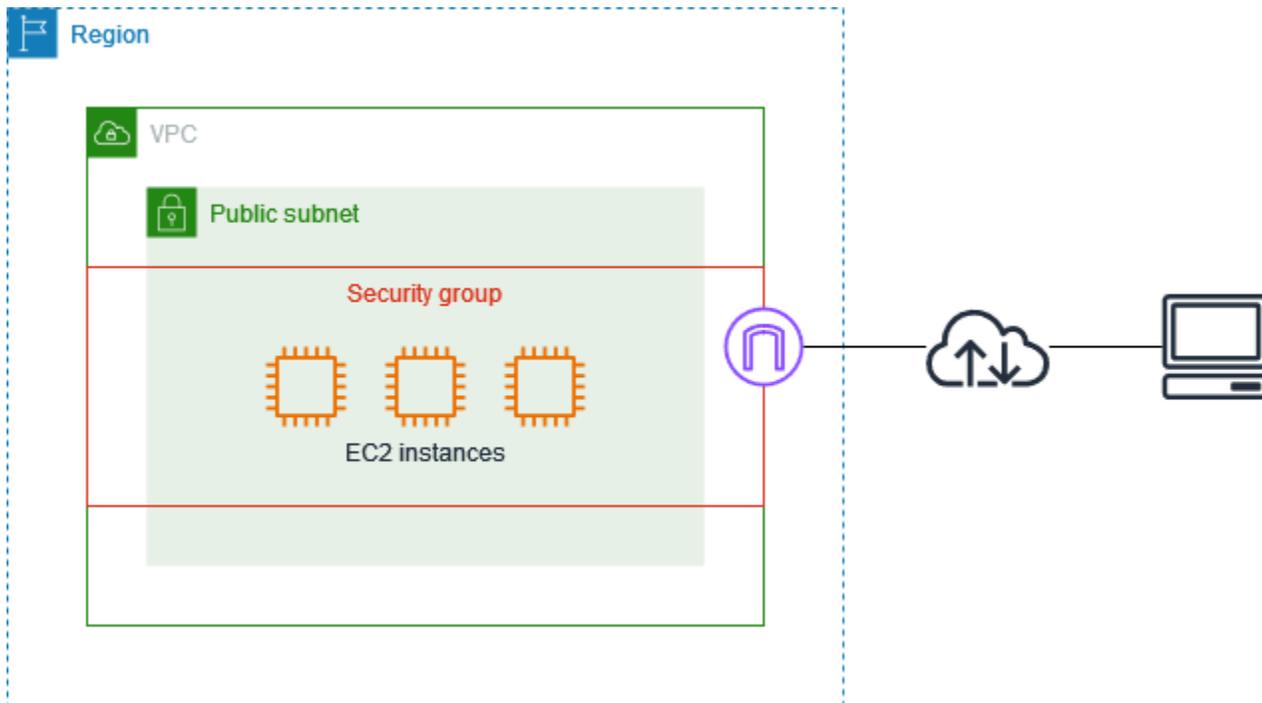
(instances Linux) Pour les paires de clés ED25519 :

```
ssh-keygen -l -f path_to_private_key
```

Groupes de sécurité Amazon EC2 pour vos instances EC2

Un groupe de sécurité agit en tant que pare-feu virtuel pour vos instances EC2 afin de contrôler le trafic entrant et sortant. Les règles entrantes contrôlent le trafic entrant vers votre instance, et les règles sortantes contrôlent le trafic sortant de votre instance. Lorsque vous lancez une instance, vous pouvez spécifier un ou plusieurs groupes de sécurité. Si vous ne spécifiez pas de groupe de sécurité, Amazon EC2 utilise le groupe de sécurité par défaut pour le VPC. Vous pouvez ajouter des règles à chaque groupe de sécurité pour autoriser le trafic vers ou depuis ses instances associées. Vous pouvez modifier les règles pour un groupe de sécurité à la fois. Les nouvelles règles sont automatiquement appliquées à toutes les instances associées au groupe de sécurité. Lorsque Amazon EC2 décide d'autoriser ou non le trafic à atteindre une instance, toutes les règles issues de tous les groupes de sécurité associés à cette instance sont évaluées automatiquement.

Le schéma suivant illustre un VPC avec un sous-réseau, une passerelle Internet et un groupe de sécurité. Le sous-réseau contient des instances EC2. Le groupe de sécurité est attribué aux instances. Le seul trafic qui atteint l'instance est le trafic autorisé par les règles du groupe de sécurité. Par exemple, si le groupe de sécurité contient une règle qui autorise le trafic SSH depuis votre réseau, vous pouvez vous connecter à votre instance depuis votre ordinateur via SSH. Si le groupe de sécurité contient une règle qui autorise tout le trafic provenant des ressources qui lui sont attribuées, chaque instance peut recevoir le trafic envoyé par les autres instances.



Après avoir lancé une instance, vous pouvez modifier ses groupes de sécurité. Les groupes de sécurité sont associés à des interfaces réseau. La modification des groupes de sécurité d'une instance change les groupes de sécurité associés à l'interface réseau principale (eth0). Pour plus d'informations, consultez [Modifier le groupe de sécurité d'une instance](#). Vous pouvez aussi modifier les groupes de sécurité associés à une autre interface réseau. Pour plus d'informations, consultez [Modifier les attributs d'interface réseau](#).

La sécurité est une responsabilité partagée entre vous AWS et vous. Pour plus d'informations, consultez [Sécurité dans Amazon EC2](#). AWS fournit des groupes de sécurité comme l'un des outils de sécurisation de vos instances, et vous devez les configurer pour répondre à vos besoins de sécurité. Si vous avez des exigences qui ne sont pas satisfaites par les groupes de sécurité, vous pouvez maintenir votre propre pare-feu sur l'une de vos instances, quelle qu'elle soit, en plus de l'utilisation des groupes de sécurité.

L'utilisation de groupes de sécurité n'entraîne aucun frais supplémentaires.

Table des matières

- [Règles des groupes de sécurité](#)
- [Suivi de connexion de groupe de sécurité](#)
- [Groupes de sécurité par défaut et personnalisés](#)
- [Utiliser des groupes de sécurité](#)

- [Règles de groupe de sécurité pour différents cas d'utilisation](#)

Règles des groupes de sécurité

Les règles d'un groupe de sécurité contrôlent le trafic entrant autorisé à atteindre les instances associées au groupe de sécurité. Les règles contrôlent également le trafic sortant autorisé à les quitter.

Les caractéristiques des règles des groupes de sécurité sont les suivantes :

- Par défaut, les groupes de sécurité contiennent des règles de sortie qui autorisent tout le trafic sortant. Vous pouvez supprimer ces règles. Notez que Amazon EC2 bloque le trafic sur le port 25 par défaut. Pour plus d'informations, consultez [Restriction sur les e-mails envoyés à l'aide du port 25](#).
- Les règles des groupes de sécurité sont toujours permissives ; vous ne pouvez pas créer de règles qui refusent l'accès.
- Les règles des groupes de sécurité vous permettent de filtrer le trafic en fonction des protocoles et des numéros de port.
- Les groupes de sécurité sont dynamiques. Si vous envoyez une demande à partir de votre instance, le trafic de la réponse à cette demande est autorisé, indépendamment des règles entrantes des groupes de sécurité. Pour les groupes de sécurité VPC, cela signifie aussi que les réponses au trafic entrant autorisé ont le droit d'être acheminées vers l'extérieur, indépendamment des règles sortantes. Pour plus d'informations, consultez [Suivi de connexion de groupe de sécurité](#).
- Vous pouvez ajouter et supprimer des règles à tout moment. Vos modifications sont appliquées automatiquement aux instances associées au groupe de sécurité.

L'effet de certaines modifications de règle peut dépendre de la manière dont le trafic est suivi. Pour plus d'informations, consultez [Suivi de connexion de groupe de sécurité](#).

- Quand vous associez plusieurs groupes de sécurité à une instance, les règles de chaque groupe de sécurité sont effectivement regroupées pour créer un seul ensemble de règles. Amazon EC2 utilise cet ensemble de règles pour déterminer si l'accès doit être autorisé ou pas.

Vous pouvez affecter plusieurs groupes de sécurité à une instance. Par conséquent, une instance peut avoir des centaines de règles qui s'appliquent. Cela peut entraîner des problèmes quand vous accédez à l'instance. Nous vous recommandons de condenser vos règles autant que possible.

Note

Les groupes de sécurité ne peuvent pas bloquer les requêtes DNS à destination ou en provenance du résolveur Route 53, parfois appelé « adresse IP VPC+2 » (voir [Qu'est-ce qu'Amazon Route 53 Resolver ?](#) dans le guide du développeur Amazon Route 53), ou le « AmazonProvided DNS » (voir [Travailler avec des ensembles d'options DHCP](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud). Si vous souhaitez filtrer les demandes DNS via Route 53 Resolver, vous pouvez activer Route 53 Resolver DNS Firewall (veuillez consulter la section [Route 53 Resolver DNS Firewall](#) du Guide du développeur Amazon Route 53).

Pour chaque règle, vous spécifiez les informations suivantes :

- Nom : nom du groupe de sécurité (par exemple, « mon-groupe-sécurité »).

Un nom peut contenir jusqu'à 255 caractères. Les caractères autorisés sont : a-z, A-Z, 0-9, espaces et `._-:/()#,@[]+=;{}!$*`. Lorsque le nom contient des espaces de fin, nous supprimons les espaces lorsque nous enregistrons le nom. Par exemple, si vous entrez « Test Security Group » pour le nom, nous le stockons comme « Test Security Group ».

- Protocole : le protocole à autoriser. Les protocoles les plus courants sont 6 (TCP) 17 (UDP) et 1 (ICMP).
- Port range (Plage de ports) : pour TCP, UDP ou un protocole personnalisé : la plage de ports autorisée. Vous pouvez spécifier un seul numéro de port (par exemple, 22), ou une plage de numéros de port (par exemple, 7000-8000).
- ICMP type and code (Type et code ICMP) : pour ICMP, le code et le type ICMP. Par exemple, utilisez le type 8 pour la requête ICMP Echo ou 128 pour la requête ICMPv6 Echo.
- Source or destination (Source ou destination) : la source (règles entrantes) ou la destination (règles sortantes) pour le trafic à autoriser. Spécifiez l'un des éléments suivants :
 - Adresse IPv4 unique. Vous devez utiliser la longueur de préfixe /32. Par exemple, 203.0.113.1/32.
 - Adresse IPv6 unique. Vous devez utiliser la longueur de préfixe /128. Par exemple, 2001:db8:1234:1a00::123/128.
 - Plage d'adresses IPv4, en notation de bloc d'adresses CIDR. Par exemple, 203.0.113.0/24.
 - Plage d'adresses IPv6, en notation de bloc d'adresses CIDR. Par exemple, 2001:db8:1234:1a00::/64.

- ID d'une liste des préfixes. Par exemple, p1-1234abc1234abc123. Pour plus d'informations, consultez [Listes de préfixes](#) dans le Amazon VPC Guide de l'utilisateur.
- ID d'un groupe de sécurité (appelé ici groupe de sécurité spécifié). Par exemple, le groupe de sécurité actuel, un groupe de sécurité du même VPC ou un groupe de sécurité pour un VPC appairé. Cela autorise le trafic basé sur les adresses IP privées des ressources associées au groupe de sécurité spécifié. Cela n'ajoute pas les règles du groupe de sécurité spécifié au groupe de sécurité actuel.
- (Facultatif) Description : vous pouvez ajouter une description pour la règle, par exemple, pour vous aider à l'identifier ultérieurement. Une description peut inclure jusqu'à 255 caractères. Les caractères autorisés sont : a-z, A-Z, 0-9, espaces et ._-:/()#,@[]+=;{}!\$*.

Lorsque vous créez une règle de groupe de sécurité, AWS attribue un identifiant unique à la règle. Vous pouvez utiliser l'ID d'une règle lorsque vous utilisez l'API ou la CLI pour modifier ou supprimer la règle.

Quand vous spécifiez un groupe de sécurité comme source ou destination d'une règle, celle-ci affecte toutes les instances associées au groupe de sécurité. Le trafic entrant est autorisé en fonction des adresses IP privées des instances associées au groupe de sécurité source (et non des adresses IP Elastic ou des adresses IP publiques). Pour plus d'informations sur les adresses IP, consultez [Adressage IP des instances Amazon EC2](#). Si votre règle de groupe de sécurité référence un groupe de sécurité supprimé dans le même VPC ou dans un VPC pair, ou référence un groupe de sécurité dans un VPC pair pour lequel la connexion d'appairage de VPC a été supprimée, la règle est marquée obsolète. Pour plus d'informations, consultez [Utilisation de règles de groupes de sécurité obsolètes](#) dans le Amazon VPC Peering Guide.

S'il existe plusieurs règles pour un port spécifique, Amazon EC2 applique la règle la plus permissive. Par exemple, si vous avez une règle qui autorise l'accès au port TCP 22 (SSH) à partir de l'adresse IP 203.0.113.1, et une autre règle qui autorise tout le monde à accéder au port TCP 22, alors tout le monde a accès au port TCP 22.

Quand vous ajoutez, mettez à jour ou supprimez des règles, les modifications sont automatiquement appliquées à toutes les instances associées au groupe de sécurité.

Suivi de connexion de groupe de sécurité

Vos groupes de sécurité utilisent le suivi de connexion pour suivre les informations sur le trafic en provenance ou à destination de l'instance. Les règles s'appliquent en fonction de l'état de connexion

du trafic pour déterminer si le trafic est autorisé ou refusé. Avec cette approche, les groupes de sécurité sont avec état. Les groupes de sécurité peuvent ainsi être avec état. Les réponses au trafic entrant sont autorisées à transiter en dehors de l'instance, indépendamment des règles sortantes des groupes de sécurité (et inversement).

À titre d'exemple, supposons que vous lanciez une commande telle que netcat ou similaire à vos instances depuis votre ordinateur personnel, et que vos règles de groupe de sécurité entrantes autorisent le trafic ICMP. Les informations sur la connexion (y compris sur le port) sont suivies. Le trafic de réponse à partir de l'instance pour la commande n'est pas suivi comme une nouvelle demande, mais plutôt comme une connexion établie, et est autorisé à circuler hors de l'instance, même si les règles de votre groupe de sécurité pour le trafic sortant limitent le trafic ICMP sortant.

Pour les protocoles autre que TCP, UDP ou ICMP, seuls l'adresse IP et le numéro de protocole sont suivis. Si votre instance envoie le trafic vers un autre hôte et que l'hôte envoie le même type de trafic vers votre instance dans un délai de 600 secondes, le groupe de sécurité de votre instance l'accepte indépendamment des règles de groupe de sécurité entrantes. Le groupe de sécurité l'accepte, car il est considéré comme un trafic de réponse pour le trafic d'origine.

Lorsque vous modifiez une règle de groupe de sécurité, ses connexions suivies ne sont pas immédiatement interrompues. Le groupe de sécurité continue d'autoriser les paquets jusqu'à l'expiration des connexions existantes. Pour vous assurer que le trafic est immédiatement interrompu ou que tout le trafic est soumis à des règles de pare-feu quel que soit l'état de suivi, vous pouvez utiliser une liste ACL réseau pour votre sous-réseau. Les ACL réseau sont sans état et n'autorisent donc pas automatiquement le trafic de réponse. L'ajout d'une liste ACL réseau qui bloque le trafic dans les deux sens interrompt les connexions existantes. Pour plus d'informations, consultez [ACL réseau](#) dans le Amazon VPC Guide de l'utilisateur.

Note

Les groupes de sécurité n'ont aucun effet sur le trafic DNS à destination ou en provenance du résolveur Route 53, parfois appelé « adresse IP VPC+2 » (voir [Qu'est-ce qu'Amazon Route 53 Resolver ?](#) dans le guide du développeur Amazon Route 53), ou le « AmazonProvided DNS » (voir [Travailler avec des ensembles d'options DHCP](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud). Si vous souhaitez filtrer les demandes DNS via Route 53 Resolver, vous pouvez activer Route 53 Resolver DNS Firewall (veuillez consulter la section [Route 53 Resolver DNS Firewall](#) du Guide du développeur Amazon Route 53).

Connexions non suivies

Certains flux de trafic ne sont pas suivis. [Si une règle de groupe de sécurité autorise les flux TCP ou UDP pour tout le trafic \(0.0.0.0/0 ou :*/0\) et qu'une règle correspondante autorise tout le trafic de réponse \(0.0.0.0/0 ou :*/0\) pour n'importe quel port \(0-65535\), ce flux de trafic n'est pas suivi, sauf s'il fait partie d'une connexion suivie automatiquement.](#) Le trafic de la réponse d'un flux non suivi est autorisé en fonction de la règle entrante ou sortante qui autorise le trafic de la réponse, et non des informations de suivi.

Un flux de trafic non suivi est immédiatement interrompu si la règle qui active le flux est supprimée ou modifiée. Par exemple, si vous disposez d'une règle sortante ouverte (0.0.0.0/0) et que vous supprimez une règle qui autorise tout le trafic SSH (port TCP 22) entrant (0.0.0.0/0) vers l'instance (ou que vous la modifiez de telle sorte que la connexion ne soit plus autorisée), vos connexions SSH existantes à l'instance sont immédiatement supprimées. La connexion n'était pas suivie auparavant, de sorte que la modificationrompt la connexion. D'autre part, si vous avez une règle entrante plus étroite qui autorise initialement une connexion SSH (ce qui signifie que la connexion a été suivie), mais que vous modifiez cette règle pour ne plus autoriser de nouvelles connexions à partir de l'adresse du client SSH actuel, la connexion SSH existante ne sera pas interrompue, car elle est suivie.

Connexions suivies automatiquement

Les connexions établies via les méthodes suivantes sont automatiquement suivies, même si la configuration du groupe de sécurité ne nécessite pas de suivi par ailleurs :

- Passerelles Internet de sortie uniquement
- Accélérateurs Global Accelerator
- Passerelles NAT
- Points de terminaison de pare-feu Network Firewall
- Network Load Balancers
- AWS PrivateLink (points de terminaison VPC d'interface)
- AWS Lambda (Interfaces réseau élastiques Hyperplane)

Allocations de suivi des connexions

Amazon EC2 définit le nombre maximal de connexions qui peuvent être suivies par instance. Une fois le maximum atteint, tous les paquets envoyés ou reçus sont abandonnés, car une nouvelle

connexion ne peut pas être établie. Lorsque cela se produit, les applications qui envoient et reçoivent des paquets ne peuvent pas communiquer correctement. Utilisez la métrique de performance réseau `conntrack_allowance_available` pour déterminer le nombre de connexions suivies encore disponibles pour ce type d'instance.

Pour déterminer si des paquets ont été abandonnés parce que le trafic réseau de votre instance a dépassé le nombre maximal de connexions pouvant être suivies, utilisez la métrique de performance réseau `conntrack_allowance_exceeded`. Pour plus d'informations, consultez [Contrôlez les performances réseau de votre instance EC2](#).

Avec Elastic Load Balancing, si vous dépassez le nombre maximal de connexions pouvant être suivies par instance, nous vous recommandons de mettre à l'échelle soit le nombre d'instances enregistrées auprès de l'équilibreur de charge, soit la taille des instances enregistrées auprès de l'équilibreur de charge.

Considérations relatives aux performances du suivi des connexions

Le routage asymétrique, selon lequel le trafic entre dans une instance via une interface réseau et sort par une interface réseau différente, peut réduire les performances maximales qu'une instance peut atteindre si les flux sont suivis.

Pour maintenir des performances optimales lorsque le suivi des connexions est activé pour vos groupes de sécurité, nous recommandons la configuration suivante :

- Évitez les topologies de routage asymétriques, si possible.
- Au lieu d'utiliser des groupes de sécurité pour le filtrage, utilisez des ACL réseau.
- Si vous devez utiliser des groupes de sécurité avec suivi des connexions, configurez le délai d'expiration de connexion le plus court possible.

Pour plus d'informations sur le réglage des performances du système Nitro, consultez [Considérations relatives au système Nitro pour le réglage des performances](#).

Délai de suivi d'inactivité de la connexion

Le groupe de sécurité assure le suivi de chaque connexion établie pour que les paquets de retour soient livrés comme prévu. Il existe un nombre maximal de connexions qui peuvent être suivies par instance. Les connexions qui restent inactives peuvent entraîner l'épuisement du suivi des connexions, empêcher le suivi des connexions et entraîner la perte de paquets. Vous pouvez définir le délai pour le suivi d'inactivité de la connexion sur une interface réseau Elastic.

Note

Cette fonctionnalité n'est disponible que pour les [instances créées sur le système AWS Nitro](#).

Il existe trois délais configurables :

- Délai TCP établi : délai d'expiration (en secondes) pour les connexions TCP inactives dans un état établi. Min. : 60 secondes. Max. : 432 000 secondes (5 jours). Par défaut : 432 000 secondes. Recommandé : moins de 432 000 secondes.
- Délai UDP : délai d'expiration (en secondes) pour les flux UDP inactifs qui n'ont vu du trafic que dans une seule direction ou une seule transaction requête-réponse. Min. : 30 secondes. Max. : 60 secondes. Par défaut : 30 secondes.
- Délai d'expiration des flux UDP : délai d'expiration (en secondes) des flux UDP inactifs classés comme des flux ayant reçu plus d'une transaction requête-réponse. Min. : 60 secondes. Max. : 180 secondes (3 minutes). Par défaut : 180 secondes.

Vous pouvez modifier les délais par défaut dans les cas suivants :

- Si vous [surveillez les connexions suivies à l'aide des métriques de performance réseau Amazon EC2](#), les métriques `contrack_allowance_exceeded` et `contrack_allowance_available` vous permettent de surveiller les paquets perdus et les connexions suivies afin de gérer de manière proactive la capacité des instances EC2 avec des actions d'augmentation ou de montée en puissance pour répondre à la demande de connexions réseau avant de perdre des paquets. Si vous observez des pertes de `contrack_allowance_exceeded` sur vos instances EC2, il peut être avantageux de définir un délai TCP plus faible pour tenir compte des sessions TCP/UDP obsolètes dues à des clients ou à des middle box réseau inappropriés.
- Généralement, les équilibreurs de charge ou les pare-feu ont un délai d'inactivité établi de TCP compris entre 60 et 90 minutes. Si vous exécutez des charges de travail censées gérer un très grand nombre de connexions (plus de 100 000) à partir d'appareils tels que des pare-feu réseau, il est conseillé de configurer un délai similaire sur une interface réseau EC2.
- Si vous exécutez une charge de travail qui utilise une topologie de routage asymétrique, nous vous recommandons de configurer un délai d'inactivité établi par TCP de 60 secondes.
- Si vous exécutez des charges de travail comportant un grand nombre de connexions telles que DNS, SIP, SNMP, Syslog, Radius et d'autres services qui utilisent principalement le protocole

UDP pour traiter les requêtes, définir le délai « flux UDP » sur 60 s permet d'augmenter la mise à l'échelle et les performances de la capacité existante et d'éviter les pannes grises.

- Pour les connexions TCP/UDP via des Network Load Balancers (NLB) et des Elastic Load Balancers (ELB), toutes les connexions sont suivies. La valeur du délai d'inactivité est de 350 secondes pour les flux TCP et de 120 secondes pour les flux UDP, et varie en fonction des valeurs de délai au niveau de l'interface. Vous souhaitez peut-être configurer les délais au niveau de l'interface réseau afin de garantir une plus grande flexibilité que les délais par défaut pour ELB/NLB.

Vous avez la possibilité de configurer les délais du suivi des connexions lorsque vous effectuez les actions suivantes :

- [Créer une interface réseau](#)
- [Modifier les attributs d'interface réseau](#)
- [Lancer une instance EC2](#)
- [Créer un modèle de lancement d'instance EC2](#)

Exemple

Dans l'exemple suivant, le groupe de sécurité dispose de règles entrantes qui autorisent le trafic TCP et ICMP, et de règles sortantes qui autorisent tout le trafic sortant.

Entrant

Type de protocole	Numéro de port	Source
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	Tous	0.0.0.0/0

Sortant

Type de protocole	Numéro de port	Destination
Tous	Tous	0.0.0.0/0
Tous	Tous	::/0

Avec une connexion réseau directe à l'instance ou à l'interface réseau, le suivi se comporte comme suit :

- Le trafic TCP entrant et sortant sur le port 22 (SSH) est suivi, car la règle de trafic entrant autorise uniquement le trafic en provenance de 203.0.113.1/32, et pas de toutes les adresses IP (0.0.0.0/0).
- Le trafic TCP entrant et sortant sur le port 80 (HTTP) n'est pas suivi, car les règles entrantes et sortantes autorisent le trafic de toutes les adresses IP.
- Le trafic ICMP est toujours suivi.

Si vous supprimez la règle sortante pour le trafic IPv4, tout le trafic IPv4 entrant et sortant est suivi, y compris le trafic sur le port 80 (HTTP). Il en va de même pour le trafic IPv6 si vous supprimez la règle sortante pour le trafic IPv6.

Groupes de sécurité par défaut et personnalisés

Votre AWS compte possède automatiquement un groupe de sécurité par défaut pour le VPC par défaut dans chaque région. Si vous ne spécifiez pas un groupe de sécurité lorsque vous lancez une instance, celle-ci est automatiquement associée au groupe de sécurité par défaut pour le VPC. Si vous ne voulez pas que vos instances utilisent le groupe de sécurité par défaut, vous pouvez créer vos propres groupes de sécurité personnalisés et les spécifier lorsque vous démarrez vos instances.

Table des matières

- [Groupes de sécurité par défaut](#)
- [Custom security groups](#)

Groupes de sécurité par défaut

Chaque VPC est associé à un groupe de sécurité par défaut. Nous vous recommandons de créer des groupes de sécurité pour des instances ou des groupes d'instances spécifiques plutôt que d'utiliser

le groupe de sécurité par défaut. Cependant, si vous ne spécifiez pas de groupe de sécurité lorsque vous lancez une instance, nous associons l'instance au groupe de sécurité par défaut pour le VPC.

Le nom d'un groupe de sécurité par défaut est « default ». Les règles par défaut d'un groupe de sécurité par défaut sont les suivantes.

Entrant

Source	Protocole	Plage de ports	Description
<i>sg-1234567890abcde</i> <i>f0</i>	Tous	Tous	Autorise le trafic entrant à partir de toutes les ressources attribuées à ce groupe de sécurité. La source est l'ID de ce groupe de sécurité.

Sortant

Destination	Protocole	Plage de ports	Description
0.0.0.0/0	Tous	Tous	Autorise tout le trafic IPv4 sortant.
::/0	Tous	Tous	Autorise tout le trafic IPv6 sortant. Cette règle est ajoutée uniquement si votre VPC dispose d'un bloc d'adresse CIDR IPv6 associé.

Principes de base des groupes de sécurité par défaut

- Vous pouvez modifier les règles du groupe de sécurité par défaut.
- Vous ne pouvez pas supprimer un groupe de sécurité par défaut. Si vous essayez de supprimer un groupe de sécurité par défaut, nous renvoyons le code d'erreur suivante : `Client.CannotDelete`.

Custom security groups

Vous pouvez créer plusieurs groupes de sécurité pour refléter les différents rôles joués par vos instances ; par exemple, des serveurs web ou des serveurs de base de données.

Quand vous créez un groupe de sécurité, vous devez lui attribuer un nom et une description. Les noms et les descriptions des groupes de sécurité peuvent comporter jusqu'à 255 caractères de long et uniquement les caractères suivants :

a-z, A-Z, 0-9, espace et `._-:/()#,@[]+=&;{}!$*`

Un nom de groupe de sécurité ne peut pas commencer par `sg-`. Un nom de groupe de sécurité doit être unique pour le VPC.

Les règles par défaut pour chaque groupe de sécurité que vous créez sont les suivantes :

- N'autorise aucun trafic entrant
- Autorise tout le trafic sortant

Après avoir créé un groupe de sécurité, vous pouvez modifier ses règles entrantes pour refléter le type de trafic entrant que vous voulez pour atteindre les instances associées. Vous pouvez aussi modifier ses règles sortantes.

Pour plus d'informations sur les règles que vous pouvez ajouter à un groupe de sécurité, consultez [Règles de groupe de sécurité pour différents cas d'utilisation](#).

Utiliser des groupes de sécurité

Vous pouvez assigner un groupe de sécurité à une instance lorsque vous lancez l'instance. Quand vous ajoutez ou supprimez des règles, ces modifications sont automatiquement appliquées à toutes les instances auxquelles vous avez affecté le groupe de sécurité. Pour plus d'informations, consultez [Affecter un groupe de sécurité à une instance](#).

Après avoir lancé une instance, vous pouvez modifier ses groupes de sécurité. Pour plus d'informations, consultez [Modifier le groupe de sécurité d'une instance](#).

Vous pouvez créer, afficher, mettre à jour et supprimer des groupes de sécurité et des règles de groupe de sécurité à l'aide de la console Amazon EC2 et des outils de ligne de commande.

Tâches

- [Création d'un groupe de sécurité](#)
- [Copier un groupe de sécurité](#)
- [Afficher vos groupes de sécurité](#)
- [Ajouter des règles à un groupe de sécurité](#)
- [Mettre à jour les règles du groupe de sécurité](#)
- [Supprimer des règles d'un groupe de sécurité](#)
- [Supprimer un groupe de sécurité](#)
- [Affecter un groupe de sécurité à une instance](#)
- [Modifier le groupe de sécurité d'une instance](#)

Création d'un groupe de sécurité

Même si vous pouvez utiliser le groupe de sécurité par défaut pour vos instances, vous souhaitez peut-être créer vos propres groupes afin de refléter les différents rôles joués par les instances dans votre système.

Par défaut, les nouveaux groupes de sécurité commencent avec seulement une règle de trafic sortant, qui permet à la totalité du trafic de quitter les instances. Vous devez ajouter des règles pour activer un trafic entrant ou limiter le trafic sortant.

Un groupe de sécurité ne peut être utilisé que dans le VPC dans lequel il est créé.

Console

Pour créer un groupe de sécurité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez Créer un groupe de sécurité.
4. Dans la section Basic details (Détails de base) procédez comme suit.
 - a. Entrez un nom descriptif et une brève description pour le groupe de sécurité. Vous ne pourrez pas les modifier une fois le groupe de sécurité créé. Le nom et la description peuvent comporter jusqu'à 255 caractères. Les caractères autorisés sont : a-z, A-Z, 0-9, espaces et `._-:/()#,@[]+=;{}!$*`.
 - b. Dans la zone VPC, choisissez le VPC.

5. Vous pouvez ajouter des règles de groupe de sécurité maintenant ou ultérieurement. Pour plus d'informations, consultez [Ajouter des règles à un groupe de sécurité](#).
6. Vous pouvez ajouter des étiquettes maintenant ou ultérieurement. Pour ajouter une étiquette, choisissez Ajouter une nouvelle étiquette), puis entrez la clé et la valeur de l'étiquette.
7. Sélectionnez Créer un groupe de sécurité.

Command line

Pour créer un groupe de sécurité

Utilisez l'une des commandes suivantes :

- [create-security-group](#) (AWS CLI)
- [New-EC2SecurityGroup](#) (AWS Tools for Windows PowerShell)

Copier un groupe de sécurité

Vous pouvez créer un nouveau groupe de sécurité en créant la copie d'un groupe existant. Lorsque vous copiez un groupe de sécurité, la copie est créée avec les mêmes règles entrantes et sortantes que le groupe de sécurité d'origine. Si le groupe de sécurité d'origine se trouve dans un VPC, la copie est créée dans le même VPC, sauf si vous en spécifiez un autre.

La copie reçoit un nouvel ID de groupe de sécurité unique et vous devez lui donner un nom. Vous pouvez également ajouter une description.

Vous ne pouvez pas copier un groupe de sécurité d'une région vers une autre région.

Vous pouvez créer une copie d'un groupe de sécurité à l'aide de la console Amazon EC2.

Pour créer un groupe de sécurité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité à copier et choisissez Actions, Copy to new security group (Copier vers un nouveau groupe de sécurité).
4. Spécifiez un nom et une description facultative, puis modifiez les règles du VPC et du groupe de sécurité si nécessaire.
5. Sélectionnez Créer.

Afficher vos groupes de sécurité

Vous pouvez afficher des informations sur vos groupes de sécurité à l'aide de l'une des méthodes suivantes.

Console

Pour afficher vos groupes de sécurité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Groupes de sécurité.
3. Vos groupes de sécurité sont répertoriés. Pour afficher les détails d'un groupe de sécurité spécifique, y compris ses règles entrantes et sortantes, choisissez son ID dans la colonne Security group ID (ID du groupe de sécurité).

Command line

Pour afficher vos groupes de sécurité

Utilisez l'une des commandes suivantes.

- [describe-security-groups](#) (AWS CLI)
- [describe-security-group-rules](#) (AWS CLI)
- [Get-EC2SecurityGroup](#) (AWS Tools for Windows PowerShell)

Amazon EC2 Global View

Vous pouvez utiliser Amazon EC2 Global View pour consulter vos groupes de sécurité dans toutes les régions pour lesquelles votre AWS compte est activé. Pour plus d'informations, consultez [Amazon EC2 Global View \(Amazon EC2 Global View\)](#).

Ajouter des règles à un groupe de sécurité

Lorsque vous ajoutez une règle à un groupe de sécurité, la nouvelle règle est automatiquement appliquée à toutes les instances associées au groupe de sécurité. Il peut y avoir un court délai avant l'application de la règle. Pour plus d'informations, consultez [Règles de groupe de sécurité pour différents cas d'utilisation](#) et [Règles des groupes de sécurité](#).

Console

Pour ajouter une règle d'entrée à un groupe de sécurité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité, puis choisissez Actions, Modifier les règles entrantes.
4. Pour chaque règle, choisissez Add rule (Ajouter une règle), puis procédez comme suit :
 - a. Pour Type, choisissez le type de protocole à autoriser.
 - Pour le protocole TCP personnalisé ou le protocole UDP personnalisé, vous devez saisir la plage de ports à autoriser. Par exemple, 0-99.
 - Pour l'ICMP personnalisé, vous devez choisir le type ICMP dans Protocole. La plage de ports est configurée pour vous. Par exemple, pour autoriser les commandes ping, choisissez Echo Request (Demande Echo) dans Protocol (Protocole).
 - Pour tous les autres types, le protocole et la plage de ports sont configurés automatiquement.
 - b. Pour Source, effectuez l'une des opérations suivantes pour autoriser le trafic.
 - Choisissez Personnalisé, puis entrez une adresse IP en notation CIDR, un bloc d'adresse CIDR, un autre groupe de sécurité ou une liste de préfixes.
 - Choisissez Anywhere pour autoriser tout le trafic du protocole spécifié à atteindre votre instance. Cette option ajoute automatiquement le bloc d'adresse CIDR IPv4 0.0.0.0/0 en tant que source. Si votre groupe de sécurité se trouve dans un VPC activé pour IPv6, cette option ajoute automatiquement une règle pour le bloc d'adresse CIDR IPv6 ::/0.

Warning

Si vous choisissez Anywhere (Partout), vous permettez à toutes les adresses IPv4 et IPv6 d'accéder à votre instance avec le protocole spécifié. Si vous ajoutez des règles pour les ports 22 (SSH) ou 3389 (RDP), vous ne devriez autoriser qu'une adresse IP ou une plage d'adresses IP spécifique à accéder à votre instance.

- Choisissez My IP (Mon IP) pour autoriser le trafic entrant uniquement à partir de l'adresse IPv4 publique de votre ordinateur local.
- c. Dans Description, vous pouvez éventuellement spécifier une description de la règle.
5. Choisissez Prévisualiser les modifications, Enregistrer les règles.

Pour ajouter une règle sortante à un groupe de sécurité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité, puis choisissez Actions, Modifier les règles sortantes.
4. Pour chaque règle, choisissez Add rule (Ajouter une règle), puis procédez comme suit :
 - a. Pour Type, choisissez le type de protocole à autoriser.
 - Pour le protocole TCP personnalisé ou le protocole UDP personnalisé, vous devez saisir la plage de ports à autoriser. Par exemple, 0-99.
 - Pour l'ICMP personnalisé, vous devez choisir le type ICMP dans Protocole. La plage de ports est configurée pour vous.
 - Pour un autre type, le protocole et la plage de ports sont configurés automatiquement.
 - b. Pour Destination, effectuez l'une des opérations suivantes.
 - Choisissez Personnalisé, puis entrez une adresse IP en notation CIDR, un bloc d'adresse CIDR ou un autre groupe de sécurité pour lequel autoriser le trafic sortant.
 - Choisissez Anywhere pour autoriser le trafic sortant vers toutes les adresses IP. Cette option ajoute automatiquement le bloc d'adresse CIDR IPv4 0.0.0.0/0 en tant que destination.

Si votre groupe de sécurité se trouve dans un VPC activé pour IPv6, cette option ajoute automatiquement une règle pour le bloc d'adresse CIDR IPv6 ::/0.
 - Choisissez My IP (Mon IP) pour autoriser le trafic sortant uniquement vers l'adresse IPv4 publique de votre ordinateur local.
 - c. (Facultatif) Pour Description, saisissez une brève description de la règle.
5. Choisissez Preview changes (Prévisualiser les modifications), Confirm (Confirmer).

Command line

Pour ajouter des règles à un groupe de sécurité

Utilisez l'une des commandes suivantes.

- [authorize-security-group-ingress](#) (AWS CLI)
- [Grant-EC2SecurityGroupIngress](#) (AWS Tools for Windows PowerShell)

Pour ajouter une ou plusieurs règles de trafic sortant à un groupe de sécurité

Utilisez l'une des commandes suivantes.

- [authorize-security-group-egress](#) (AWS CLI)
- [Grant-EC2SecurityGroupEgress](#) (AWS Tools for Windows PowerShell)

Mettre à jour les règles du groupe de sécurité

Vous pouvez mettre à jour une règle de groupe de sécurité à l'aide de l'une des méthodes suivantes. La règle mise à jour est automatiquement appliquée à toutes les instances associées au groupe de sécurité.

Console

Lorsque vous modifiez le protocole, la plage de ports, ou la source ou destination de la règle existante d'un groupe de sécurité à l'aide de la console, cette dernière supprime la règle existante et en ajoute une nouvelle.

Pour mettre à jour un groupe de sécurité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité.
4. Choisissez Actions, puis Edit inbound rules (Modifier les règles entrantes) pour mettre à jour une règle pour le trafic entrant ou Actions, puis Edit outbound rules (Modifier les règles sortantes) pour mettre à jour une règle pour le trafic sortant.
5. Mettez à jour la règle comme requis.
6. Choisissez Preview changes (Prévisualiser les modifications), Confirm (Confirmer).

Pour étiqueter une règle de groupe de sécurité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité.
4. Sous l'onglet Règles entrantes ou Règles sortantes, sélectionnez la case à cocher de la règle, puis choisissez Gérer les étiquettes.
5. La page Gérer les étiquettes affiche toutes les étiquettes affectées à la règle. Pour ajouter une étiquette, choisissez Ajouter une étiquette, puis entrez la clé et la valeur de l'étiquette. Pour supprimer une balise, choisissez Remove (Supprimer) en regard de la balise à supprimer.
6. Sélectionnez Save changes (Enregistrer les modifications).

Command line

Vous ne pouvez pas modifier le protocole, la plage de ports, ou la source ou destination de la règle existante d'un groupe de sécurité à l'aide de l'API Amazon EC2 ou d'un outil de ligne de commande. Vous devez plutôt supprimer la règle existante, puis ajouter une nouvelle règle. Vous pouvez toutefois mettre à jour la description d'une règle existante.

Pour mettre à jour une règle

Utilisez la commande suivante.

- [modify-security-group-rules](#) (AWS CLI)

Pour mettre à jour la description d'une règle entrante existante

Utilisez l'une des commandes suivantes.

- [update-security-group-rule-descriptions-ingress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleIngressDescription](#) (AWS Tools for Windows PowerShell)

Pour mettre à jour la description d'une règle sortante existante

Utilisez l'une des commandes suivantes.

- [update-security-group-rule-descriptions-egress](#) (AWS CLI)

- [Update-EC2SecurityGroupRuleEgressDescription](#) (AWS Tools for Windows PowerShell)

Pour étiqueter une règle de groupe de sécurité

Utilisez l'une des commandes suivantes.

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)

Supprimer des règles d'un groupe de sécurité

Lorsque vous supprimez une règle d'un groupe de sécurité, la modification est automatiquement appliquée à toutes les instances associées au groupe de sécurité.

Vous pouvez supprimer des règles d'un groupe de sécurité à l'aide de l'une des méthodes suivantes.

Console

Pour supprimer une règle de groupe de sécurité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité à mettre à jour, choisissez Actions, puis choisissez Edit inbound rules (Modifier les règles entrantes) pour supprimer une règle entrante ou Edit outbound rules (Modifier les règles sortantes) pour supprimer une règle sortante.
4. Cliquez sur le bouton Delete (Supprimer) à droite de la règle à supprimer.
5. Sélectionnez Enregistrer les règles. Vous pouvez également choisir Prévisualiser les modifications, vérifier vos modifications, puis cliquer sur Confirmer.

Command line

Supprimer une ou plusieurs règles de trafic entrant d'un groupe de sécurité

Utilisez l'une des commandes suivantes.

- [revoke-security-group-ingress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupIngress](#) (AWS Tools for Windows PowerShell)

Pour supprimer une ou plusieurs règles de trafic sortant d'un groupe de sécurité

Utilisez l'une des commandes suivantes.

- [revoke-security-group-egress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupEgress](#) (AWS Tools for Windows PowerShell)

Supprimer un groupe de sécurité

Vous ne pouvez pas supprimer un groupe de sécurité associé à une instance. Vous ne pouvez pas supprimer le groupe de sécurité par défaut. Vous ne pouvez pas supprimer un groupe de sécurité référencé par un autre groupe de sécurité dans le même VPC. Si votre groupe de sécurité est référencé par l'une de ses propres règles, vous devez supprimer la règle avant de pouvoir supprimer le groupe de sécurité.

Console

Pour supprimer un groupe de sécurité

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité, puis choisissez Actions, Supprimer les groupes de sécurité.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Command line

Pour supprimer un groupe de sécurité

Utilisez l'une des commandes suivantes.

- [delete-security-group](#) (AWS CLI)
- [Remove-EC2SecurityGroup](#) (AWS Tools for Windows PowerShell)

Affecter un groupe de sécurité à une instance

Vous pouvez affecter un ou plusieurs groupes de sécurité à une instance lorsque vous lancez l'instance. Vous pouvez également spécifier un ou plusieurs groupes de sécurité dans un modèle de

lancement. Les groupes de sécurité sont affectés à toutes les instances lancées à l'aide du modèle de lancement.

- Pour affecter un groupe de sécurité à une instance lorsque vous lancez l'instance, consultez [Paramètres réseau](#) de [Lancer une instance à l'aide de paramètres définis](#) (nouvelle console) ou [Étape 6 : Configurer un groupe de sécurité](#) (ancienne console).
- Pour spécifier un groupe de sécurité dans un modèle de lancement, consultez [Paramètres réseau](#) de [Création d'un modèle de lancement à partir de paramètres](#).

Modifier le groupe de sécurité d'une instance

Après avoir lancé une instance, vous pouvez modifier ses groupes de sécurité en ajoutant ou en supprimant des groupes de sécurité.

Prérequis

- L'instance doit être dans l'état `running` ou `stopped`.
- Un groupe de sécurité est spécifique à un VPC. Vous pouvez affecter un groupe de sécurité à une ou plusieurs instances lancées dans le VPC pour lequel vous avez créé le groupe de sécurité.

Console

Pour changer les groupes de sécurité d'une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez votre instance, puis Actions (Actions), Security (Sécurité), Change security groups (Modifier les groupes de sécurité).
4. Pour Associated security groups (Groupes de sécurité associés), sélectionnez un groupe de sécurité dans la liste et choisissez Add security group (Ajouter un groupe de sécurité).

Pour supprimer un groupe de sécurité déjà associé, choisissez Remove (Supprimer) pour ce groupe de sécurité.

5. Choisissez Enregistrer.

Command line

Pour changer les groupes de sécurité d'une instance

Utilisez l'une des commandes suivantes.

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

Règles de groupe de sécurité pour différents cas d'utilisation

Vous pouvez créer un groupe de sécurité et ajouter des règles qui reflètent le rôle de l'instance qui est associée à ce groupe. Par exemple, une instance configurée en tant que serveur web nécessite des règles de groupe de sécurité qui autorisent l'accès HTTP et HTTPS entrant. De même, une instance de base de données a besoin de règles permettant l'accès au type de base de données, telles que l'accès via le port 3306 pour MySQL.

Voici des exemples de types de règles que vous pouvez ajouter à des groupes de sécurité pour des types d'accès spécifiques.

Exemples

- [Règles de serveur web](#)
- [Règles de serveur de base de données](#)
- [Règles pour la connexion à des instances à partir de votre ordinateur](#)
- [Règles pour la connexion à des instances à partir d'une instance avec le même groupe de sécurité](#)
- [Règles pour Ping/ICMP](#)
- [Règles de serveur DNS](#)
- [Règles Amazon EFS](#)
- [Règles Elastic Load Balancing](#)
- [Règles d'appairage de VPC](#)

Règles de serveur web

Les règles entrantes suivantes autorisent l'accès HTTP et HTTPS à partir de n'importe quelle adresse IP. Si votre VPC est activé pour IPv6, vous pouvez ajouter des règles pour contrôler le trafic HTTP et HTTPS entrant à partir d'adresses IPv6.

Type de protocole	Numéro de protocole	Port	IP Source	Remarques
TCP	6	80 (HTTP)	0.0.0.0/0	Autorise l'accès HTTP entrant à partir de n'importe quelle adresse IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Autorise l'accès HTTPS entrant à partir de n'importe quelle adresse IPv4
TCP	6	80 (HTTP)	::/0	Autorise l'accès HTTP entrant à partir de n'importe quelle adresse IPv6.
TCP	6	443 (HTTPS)	::/0	Autorise l'accès HTTPS entrant à partir de n'importe quelle adresse IPv6.

Règles de serveur de base de données

Les règles entrantes suivantes sont des exemples de règles que vous pouvez ajouter pour un accès à une base de données selon le type de base de données que vous exécutez sur votre instance.

Pour plus d'informations sur les instances Amazon RDS, consultez le [Guide de l'utilisateur Amazon RDS](#).

Pour l'adresse IP source, spécifiez l'une des options suivantes :

- Une adresse IP spécifique ou une plage d'adresses IP (en notation de bloc CIDR) de votre réseau local
- Un ID de groupe de sécurité pour un groupe d'instances qui accèdent à la base de données

Type de protocole	Numéro de protocole	Port	Remarques
TCP	6	1433 (MS SQL)	Port par défaut pour accéder à une base de données Microsoft

Type de protocole	Numéro de protocole	Port	Remarques
			SQL Server, par exemple, sur une instance Amazon RDS
TCP	6	3306 (MYSQL/Aurora)	Port par défaut pour accéder à une base MySQL ou Aurora, par exemple, sur une instance Amazon RDS
TCP	6	5439 (Redshift)	Port par défaut pour accéder à une base de données de cluster Amazon Redshift.
TCP	6	5432 (PostgreSQL)	Port par défaut pour accéder à une base de données PostgreSQL, par exemple, sur une instance Amazon RDS
TCP	6	1521 (Oracle)	Port par défaut pour accéder à une base de données Oracle, par exemple, sur une instance Amazon RDS

Vous pouvez éventuellement restreindre le trafic sortant de vos serveurs de base de données. Par exemple, vous pouvez autoriser l'accès à Internet pour les mises à jour logicielles, mais limiter tous les autres types de trafic. Vous devez d'abord supprimer la règle sortante par défaut qui autorise tout le trafic sortant.

Type de protocole	Numéro de protocole	Port	IP de destination	Remarques
TCP	6	80 (HTTP)	0.0.0.0/0	Autorise l'accès HTTP sortant vers toute adresse IPv4

Type de protocole	Numéro de protocole	Port	IP de destination	Remarques
TCP	6	443 (HTTPS)	0.0.0.0/0	Autorise l'accès HTTPS sortant vers toute adresse IPv4
TCP	6	80 (HTTP)	::/0	(VPC activé pour IPv6 uniquement) Autorise l'accès HTTP sortant vers toute adresse IPv6
TCP	6	443 (HTTPS)	::/0	(VPC activé pour IPv6 uniquement) Autorise l'accès HTTPS sortant vers toute adresse IPv6

Règles pour la connexion à des instances à partir de votre ordinateur

Pour se connecter à votre instance, votre groupe de sécurité doit avoir des règles entrantes qui autorisent l'accès SSH (pour les instances Linux) ou l'accès RDP (pour les instances Windows).

Type de protocole	Numéro de protocole	Port	IP Source
TCP	6	22 (SSH)	Adresse IPv4 publique de votre ordinateur, ou une plage d'adresses IP de votre réseau local. Si votre VPC est activé pour IPv6 et que votre instance a une adresse IPv6, vous pouvez entrer une adresse ou une plage d'adresses IPv6.
TCP	6	3389 (RDP)	Adresse IPv4 publique de votre ordinateur, ou une plage d'adresses IP de votre réseau local. Si votre VPC est activé pour IPv6 et que votre

Type de protocole	Numéro de protocole	Port	IP Source
			instance a une adresse IPv6, vous pouvez entrer une adresse ou une plage d'adresses IPv6.

Règles pour la connexion à des instances à partir d'une instance avec le même groupe de sécurité

Pour autoriser les instances associées au même groupe de sécurité à communiquer les unes avec les autres, vous devez à cette fin ajouter des règles explicitement.

Note

Si vous configurez des acheminements pour transférer le trafic entre deux instances de sous-réseaux différents via une appliance middlebox, vous devez vous assurer que les groupes de sécurité des deux instances autorisent le trafic à transiter entre les instances. Le groupe de sécurité de chaque instance doit référencer l'adresse IP privée de l'autre instance ou la plage d'adresses CIDR du sous-réseau qui contient l'autre instance en tant que source. Si vous référencez le groupe de sécurité de l'autre instance en tant que source, cela n'autorise pas le trafic à transiter entre les instances.

Le tableau suivant décrit la règle entrante pour un groupe de sécurité qui permet aux instances associées de communiquer les unes avec les autres. La règle autorise tous les types de trafic.

Type de protocole	Numéro de protocole	Ports	IP Source
-1 (Tout)	-1 (Tout)	-1 (Tout)	L'ID du groupe de sécurité, ou la plage d'adresses CIDR du sous-réseau qui contient l'autre instance (voir note).

Règles pour Ping/ICMP

La commande ping est un type de trafic ICMP. Pour envoyer une commande ping à votre instance, vous devez ajouter l'une des règles ICMP entrantes suivantes.

Type	Protocole	Source		
ICMP personnalisé - IPv4	Demande Echo	L'adresse IPv4 publique de votre ordinateur, une adresse IPv4 spécifique ou une adresse IPv4 ou IPv6 de n'importe où.		
Tous les ICMP - IPv4	ICMP IPv4 (1)	L'adresse IPv4 publique de votre ordinateur, une adresse IPv4 spécifique ou une adresse IPv4 ou IPv6 de n'importe où.		

Pour utiliser la commande ping6 afin d'effectuer un test ping sur l'adresse IPv6 pour votre instance, vous devez ajouter la règle ICMPv6 entrante suivante.

Type	Protocole	Source		
Tous les ICMP - IPv6	ICMP IPv6 (58)	L'adresse IPv6 de votre ordinateur, une adresse IPv4 spécifique ou une adresse		

Type	Protocole	Source		
		IPv4 ou IPv6 de n'importe où.		

Règles de serveur DNS

Si vous avez configuré votre instance EC2 en tant que serveur DNS, vous devez vous assurer que le trafic TCP et UDP peut accéder à votre serveur DNS via le port 53.

Pour l'adresse IP source, spécifiez l'une des options suivantes :

- Adresse IP ou plage d'adresses IP (en notation de bloc CIDR) d'un réseau
- L'ID d'un groupe de sécurité pour l'ensemble d'instances de votre réseau devant accéder au serveur DNS

Type de protocole	Numéro de protocole	Port
TCP	6	53
UDP	17	53

Règles Amazon EFS

Si vous utilisez un système de fichiers Amazon EFS avec vos instances Amazon EC2, le groupe de sécurité que vous associez à vos cibles de montage Amazon EFS doit autoriser le trafic via le protocole NFS.

Type de protocole	Numéro de protocole	Ports	IP Source	Remarques
TCP	6	2049 (NFS)	ID du groupe de sécurité	Autorise l'accès NFS entrant à partir des ressources (y compris la cible de montage)

Type de protocole	Numéro de protocole	Ports	IP Source	Remarques
				associées à ce groupe de sécurité.

Pour monter un système de fichiers Amazon EFS sur votre instance Amazon EC2 vous devez vous connecter à votre instance. Par conséquent, le groupe de sécurité associé à votre instance doit avoir des règles qui autorisent le trafic SSH entrant à partir de votre ordinateur local ou de votre réseau local.

Type de protocole	Numéro de protocole	Ports	IP Source	Remarques
TCP	6	22 (SSH)	Plage d'adresses IP de votre ordinateur local ou plage d'adresses IP (en notation de bloc CIDR) de votre réseau.	Autorise l'accès SSH entrant depuis votre ordinateur local.

Règles Elastic Load Balancing

Si vous utilisez un équilibreur de charge, le groupe de sécurité associé à celui-ci doit avoir des règles qui autorisent la communication avec vos instances ou cibles. Pour plus d'informations, consultez [Configurer des groupes de sécurité pour votre Classic Load Balancer](#) dans le Guide de l'utilisateur pour les Classic Load Balancer et [Groupes de sécurité pour votre Application Load Balancer](#) dans le Guide de l'utilisateur pour les Application Load Balancer.

Règles d'appairage de VPC

Vous pouvez mettre à jour les règles entrantes ou sortantes pour les groupes de sécurité de votre VPC pour référencer des groupes de sécurité dans le VPC appairé. Cette étape autorise la circulation du trafic vers et depuis les instances associées au groupe de sécurité référencé dans le VPC appairé. Pour plus d'informations sur la configuration des groupes de sécurité pour l'appairage de VPC, consultez [Mise à jour de vos groupes de sécurité pour référencer les groupes de VPC pairs](#).

NitroTPM

Nitro Trusted Platform Module (NitroTPM) est un périphérique virtuel fourni par l'[AWS Nitro System](#) et est conforme aux [spécifications TPM 2.0](#). Il stocke en toute sécurité les artefacts (tels que les mots de passe, les certificats ou les clés de chiffrement) utilisés pour authentifier l'instance. NitroTPM peut générer des clés et les utiliser pour des fonctions cryptographiques (telles que le hachage, la signature, le chiffrement et le déchiffrement).

NitroTPM assure un démarrage mesuré, un processus lors duquel le chargeur de démarrage et le système d'exploitation créent des hachages cryptographiques de chaque binaire de démarrage et les combinent avec les valeurs précédentes des registres de configuration de plateforme (PCR) internes NitroTPM. Avec le démarrage mesuré, vous pouvez obtenir des valeurs PCR signées de NitroTPM et les utiliser pour prouver aux entités distantes l'intégrité du logiciel de démarrage de l'instance. Cela porte le nom d'attestation distante.

Avec NitroTPM, les clés et les secrets peuvent être étiquetés avec une valeur PCR spécifique ; ce faisant, leur accès est interdit en cas de modification de la valeur de la PCR, et donc de l'intégrité de l'instance. Cette forme spéciale d'accès conditionnel est appelée scellement et descellement. Les technologies des systèmes d'exploitation [BitLocker](#), telles que NitroTPM, peuvent utiliser NitroTPM pour sceller une clé de déchiffrement du lecteur afin que le lecteur ne puisse être déchiffré que lorsque le système d'exploitation a démarré correctement et est dans un état connu comme bon.

Pour utiliser NitroTPM, vous devez sélectionner une [image machine Amazon](#) (AMI) configurée pour prendre en charge NitroTPM, puis utiliser l'AMI pour lancer des [instances basées sur](#) le système Nitro. AWS Vous pouvez sélectionner l'une des AMI prédéfinies d'Amazon ou en créer une vous-même.

Coûts

L'utilisation de NitroTPM n'entraîne aucun coût supplémentaire. Vous payez uniquement les ressources sous-jacentes que vous utilisez.

Rubriques

- [Considérations](#)
- [Conditions préalables à l'activation au lancement](#)
- [Créer une AMI Linux pour la prise en charge de NitroTPM](#)
- [Vérifiez si une AMI est activée pour NitroTPM](#)

- [Activer ou arrêter l'utilisation de NitroTPM sur une instance](#)
- [Récupérer la clé d'approbation publique pour une instance](#)

Considérations

Les considérations suivantes s'appliquent lorsque vous utilisez NitroTPM :

- BitLocker les volumes chiffrés à l'aide de clés basées sur NitroTPM ne peuvent être utilisés que sur l'instance d'origine.
- L'état NitroTPM n'est pas inclus dans les [instantanés Amazon EBS](#).
- L'état NitroTPM n'est pas inclus dans les images [VM Import/Export](#).
- La prise en charge NitroTPM est activée lorsqu'une valeur de `v2.0` est spécifiée pour le paramètre `tpm-support` lors de la création d'une AMI. Après avoir lancé une instance avec l'AMI, vous ne pouvez pas modifier les attributs de l'instance. Les instances dotées de NitroTPM ne prennent pas en charge l'API [ModifyInstanceAttribute](#).
- Vous pouvez uniquement créer une AMI avec NitroTPM configuré à l'aide de l'[RegisterImageAPI](#) en utilisant la console Amazon EC2 AWS CLI et non avec celle-ci.
- NitroTPM n'est pas pris en charge sur Outposts.
- NitroTPM n'est pas pris en charge dans les zones locales ou les zones Wavelength.

Conditions préalables à l'activation au lancement

Pour lancer une instance avec NitroTPM activé, les conditions préalables suivantes doivent être réunies.

Instances Linux

AMI

Nécessite une AMI pour laquelle NitroTPM est activé.

Actuellement, il n'existe aucune AMI Amazon Linux dans laquelle NitroTPM est activé. Pour utiliser une AMI supportée, vous devez effectuer plusieurs étapes de configuration sur votre propre AMI Linux. Pour plus d'informations, consultez [Créer une AMI Linux pour la prise en charge de NitroTPM](#).

Système d'exploitation

L'AMI doit inclure un système d'exploitation doté d'un pilote Command Response Buffer (CRB) TPM 2.0. La plupart des systèmes d'exploitation actuels, tels qu'Amazon Linux 2, contiennent un pilote CRB TPM 2.0.

Mode de démarrage UEFI

NitroTPM requiert qu'une instance soit exécutée en mode de démarrage UEFI, ce qui nécessite que l'AMI soit configurée pour le mode de démarrage UEFI. Pour plus d'informations, consultez [UEFI Secure Boot](#).

instances Windows

AMI

Nécessite une AMI pour laquelle NitroTPM est activé.

Les AMI Windows suivantes sont préconfigurées pour activer NitroTPM et UEFI Secure Boot avec des clés Microsoft :

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise
- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

Actuellement, l'importation sur Windows avec NitroTPM à l'aide de la commande [import-image](#) n'est pas prise en charge.

Système d'exploitation

L'AMI doit inclure un système d'exploitation doté d'un pilote Command Response Buffer (CRB) TPM 2.0. La plupart des systèmes d'exploitation actuels, tels que TPM-Windows_Server-2_English-Full-Base, contiennent un pilote CRB TPM 2.0.

Mode de démarrage UEFI

NitroTPM requiert qu'une instance soit exécutée en mode de démarrage UEFI, ce qui nécessite que l'AMI soit configurée pour le mode de démarrage UEFI. Pour plus d'informations, consultez [UEFI Secure Boot](#).

Types d'instances

Vous devez utiliser l'un des types d'instances virtualisées suivants :

- Usage général : M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7i, M7i-Flex, T3, T3a
- Optimisé pour le calcul : C5, C5a, C5ad, C5d, C5n, C6a, C6i, C6id, C6in, C7a, C7i, C7i-Flex
- Mémoire optimisée : R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7i, R7iZ, U7i-12TB, U7in-16TB, U7in-32TB, X2IDN, X2iEDN, x2ieZn, z1d
- Stockage optimisé : D3, D3en, i3EN, i4i
- Calcul accéléré : G4dn, G5, G6, Gr6, Inf1, Inf2
- Calcul à hautes performances : HPC6a, HPC6id

Note

Les instances basées sur Graviton, les instances Xen, les instances Mac et les instances bare metal ne sont pas prises en charge.

Créer une AMI Linux pour la prise en charge de NitroTPM

Lors de l'enregistrement de votre AMI, vous devez configurer votre AMI Linux pour qu'elle soit prise en charge par NitroTPM. Vous ne pouvez pas configurer la prise en charge NitroTPM ultérieurement.

Pour obtenir la liste des AMI Windows préconfigurées pour la prise en charge de NitroTPM, consultez [Conditions préalables à l'activation au lancement](#)

Pour enregistrer une AMI Linux pour le support de NitroTPM

1. Lancez une instance temporaire avec l'AMI Linux requise.

2. Une fois que l'instance a atteint `running` cet état, créez un instantané du volume racine de l'instance.
3. Enregistrez la nouvelle AMI. Utilisez la commande [register-image](#). Pour `--tpm-support`, spécifiez `v2.0`. Pour `--boot-mode`, spécifiez `uefi`. Et spécifiez un mappage de périphériques en mode bloc pour le volume racine à l'aide de l'instantané que vous avez créé à l'étape précédente.

```
aws ec2 register-image \  
  --name my-image \  
  --boot-mode uefi \  
  --architecture x86_64 \  
  --root-device-name /dev/xvda \  
  --block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=snapshot_id} \  
  --tpm-support v2.0
```

Sortie attendue

```
{  
  "ImageId": "ami-0123456789example"  
}
```

4. Mettez fin à l'instance temporaire que vous avez lancée à l'étape 1, si elle n'est plus nécessaire.

Vérifiez si une AMI est activée pour NitroTPM

Vous pouvez utiliser `describe-images` ou `describe-image-attributes` pour vérifier si une AMI est activée pour NitroTPM.

Pour vérifier si une AMI est activée pour NitroTPM à l'aide de **`describe-images`**

Utilisez la commande [describe-images](#) et spécifiez l'ID de l'AMI.

```
aws ec2 describe-images --image-ids ami-0123456789example
```

Si NitroTPM est activé pour l'AMI, `"TpmSupport": "v2.0"` s'affiche.

```
{  
  "Images": [  
    {
```

```
    ...
    "BootMode": "uefi",
    ...
    "TpmSupport": "v2.0"
  }
]
}
```

Pour vérifier si une AMI est activée pour NitroTPM à l'aide de **describe-image-attribute**

Utilisez la commande [describe-image-attribute](#) et spécifiez le paramètre `attribute` avec la valeur `tpmSupport`.

Note

Vous devez être le propriétaire de l'AMI pour appeler `describe-image-attribute`.

```
aws ec2 describe-image-attribute \
  --region us-east-1 \
  --image-id ami-0123456789example \
  --attribute tpmSupport
```

Si NitroTPM est activé pour l'AMI, la valeur de `TpmSupport` est `"v2.0"`. Notez que `describe-image-attribute` renvoie uniquement les attributs spécifiés dans la demande.

```
{
  "ImageId": "ami-0123456789example",
  "TpmSupport": {
    "Value": "v2.0"
  }
}
```

Activer ou arrêter l'utilisation de NitroTPM sur une instance

Lorsque vous lancez une instance à partir d'une AMI pour laquelle la prise en charge par NitroTPM est activée, l'instance est lancée et NitroTPM est activé. Vous pouvez configurer l'instance pour qu'elle cesse d'utiliser NitroTPM. Vous pouvez vérifier si une instance est activée pour NitroTPM.

Rubriques

- [Lancer une instance pour laquelle NitroTPM est activé](#)
- [Arrêter l'utilisation de NitroTPM sur une instance](#)
- [Vérifier si NitroTPM est accessible au sein de l'instance](#)

Lancer une instance pour laquelle NitroTPM est activé

Lorsque vous lancez une instance selon les [prérequis](#), NitroTPM est automatiquement activé sur l'instance. Vous pouvez uniquement activer NitroTPM sur une instance au lancement. Pour plus d'informations sur le lancement d'une instance, consultez [Lancer votre instance](#).

Arrêter l'utilisation de NitroTPM sur une instance

Après avoir lancé une instance pour laquelle NitroTPM est activé, vous ne pouvez pas désactiver NitroTPM pour cette instance. Toutefois, vous pouvez configurer le système d'exploitation pour qu'il cesse d'utiliser NitroTPM en désactivant le pilote de périphérique TPM 2.0 sur l'instance à l'aide des outils suivants :

- [Instances Linux] Utilisez tpm-tools.
- [Instances Windows] Utilisez la console de gestion du TPM, tpm.msc.

Pour plus d'informations sur la désactivation du pilote de périphérique, consultez la documentation de votre système d'exploitation.

Vérifier si NitroTPM est accessible au sein de l'instance

Pour vérifier si une instance est activée pour la prise en charge de NitroTPM à l'aide du AWS CLI

Utilisez la commande [describe-instances](#) AWS CLI et spécifiez l'ID de l'instance. Actuellement, la console Amazon EC2 n'affiche pas le champ TpmSupport.

```
aws ec2 describe-instances --instance-ids i-0123456789example
```

Si NitroTPM est activé pour l'instance, "TpmSupport": "v2.0" s'affiche.

```
"Instances": {  
  "InstanceId": "0123456789example",  
  "InstanceType": "c5.large",  
  ...  
  "BootMode": "uefi",
```

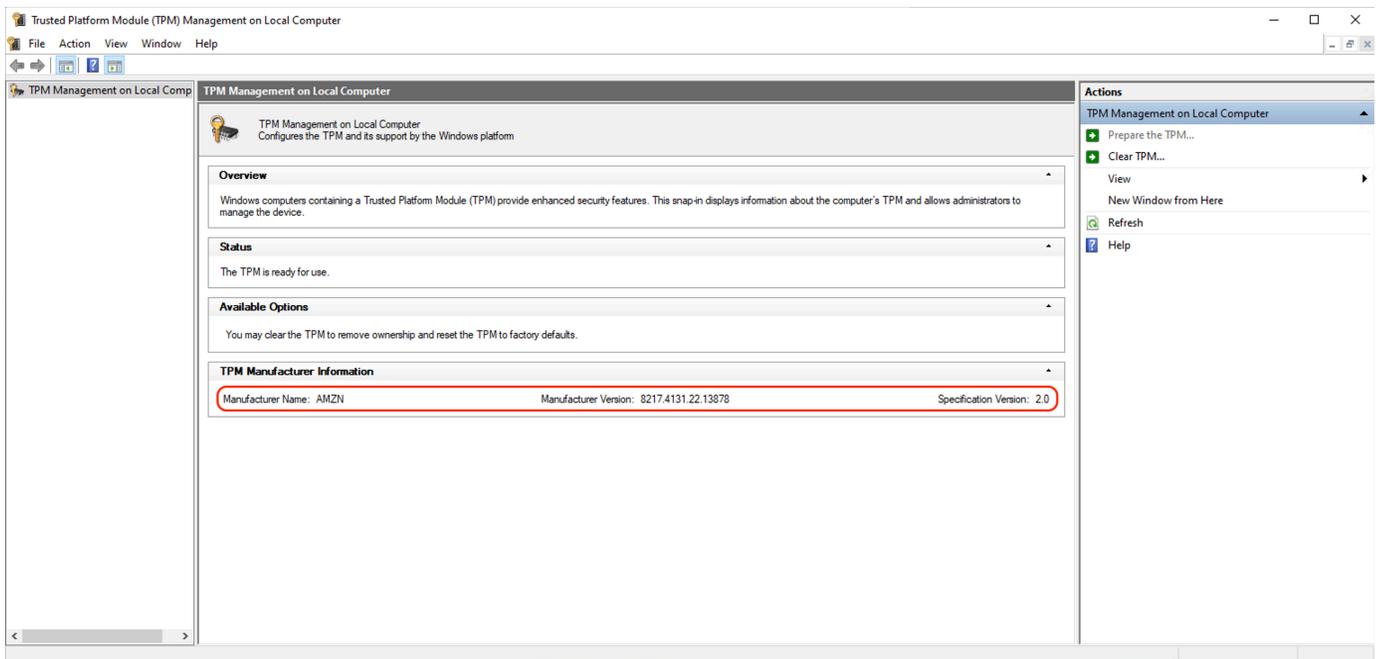
```
"TpmSupport": "v2.0"  
...  
}
```

(instances Windows) Pour vérifier si NitroTPM est accessible dans une instance Windows Amazon EC2

1. [Connectez-vous à votre instance EC2 Windows.](#)
2. Sur l'instance, exécutez le programme tpm.msc.

La fenêtre TPM Management on Local Computer (Gestion TPM sur un ordinateur local) s'ouvre.

3. Vérifiez le champ TPM Manufacturer Information (Informations sur le fabricant TPM). Il contient le nom du fabricant et la version du NitroTPM sur l'instance.



Récupérer la clé d'approbation publique pour une instance

Vous pouvez récupérer en toute sécurité la clé d'approbation publique d'une instance à tout moment à l'aide du AWS CLI.

Pour récupérer la clé d'approbation publique pour une instance

Utilisez la AWS CLI commande [get-instance-tpm-ek-pub](#).

Exemple 1

L'exemple de commande suivant obtient la clé d'approbation `rsa-2048` publique au `tpmt` format par exemple `i-01234567890abcdef`.

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format tpmt \
--key-type rsa-2048
```

Voici un exemple de sortie.

```
{
  "InstanceId": "i-01234567890abcdef",
  "KeyFormat": "tpmt",
  "KeyType": "rsa-2048",
  "KeyValue": "AAEACwADALIAIINx12dEhLEXAMPLEUa11yT9UtduB1ILZPKh2hszFGmqAAYAgABDA
EXAMPLEAAABA0iRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0L0LiYnEXAMPLERqApiFa/UhvEYqN4
Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDth1S7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
0S1ZtNuItMs+Yp4S06aU28MT/JZk0KsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgv00QTTJVGDxh
vxtXC0u9GYf0crbjEXAMPLEd4YTbWdDdg0KWF9fjzDytJSDhrLA0UctNzHPCd/9215zEXAMPLE0IFA
Ss50C0/802c17W2pMSVHvCCa91YCiAfxH/vYKovAAE="
}
```

Exemple 2

L'exemple de commande suivant obtient la clé d'approbation `rsa-2048` publique au `der` format par exemple `i-01234567890abcdef`.

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format der \
--key-type rsa-2048
```

Voici un exemple de sortie.

```
{
  "InstanceId": "i-01234567890abcdef",
  "KeyFormat": "der",
  "KeyType": "rsa-2048",
  "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DgzB4
JcTFuUbykRR82bQs4uJifaKS0v5NGoEXAMPLEEG8Rio3hnuMowP+6xuGxBoAHWAoD1Gb06FJrMdEXAMP
LEnYUHVm02GVLsc0a5ifl4buqcnd1FqxRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP81mQ4qxch0x6
```

```
tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNM1UZ0PGG/G1cI670Zh/Rytu0dx9iEXAMPLEtZ0N2A4pYX  
1+PMPK01I0GssA5Ry03Mc8J3/3aXn0D2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi  
8AAQIDAQAB"  
}
```

Credential Guard pour les instances Windows

Le système AWS Nitro prend en charge Credential Guard pour les instances Windows Amazon Elastic Compute Cloud (Amazon EC2). Credential Guard est une fonction de sécurité basée sur la virtualisation (VBS) de Windows qui permet de créer des environnements isolés pour protéger les ressources de sécurité, telles que les informations d'identification des utilisateurs Windows et l'application de l'intégrité du code, au-delà des protections du noyau Windows. Lorsque vous exécutez des instances Windows EC2, Credential Guard utilise le système AWS Nitro pour empêcher l'extraction des informations de connexion Windows de la mémoire du système d'exploitation.

Table des matières

- [Prérequis](#)
- [Lancer une instance prise en charge](#)
- [Désactiver l'intégrité de la mémoire](#)
- [Activez Credential Guard](#)
- [Vérifiez que Credential Guard est en cours d'exécution](#)

Prérequis

Votre instance Windows doit remplir les conditions préalables suivantes pour utiliser Credential Guard :

Amazon Machine Images (AMI)

L'AMI doit être préconfigurée pour activer NitroTPM et UEFI Secure Boot. Pour plus d'informations sur les AMI prises en charge, consultez [the section called "Prérequis"](#).

Intégrité de la mémoire

L'intégrité de la mémoire, également appelée intégrité du code protégée par l'hyperviseur (HVCI) ou intégrité du code appliquée à l'hyperviseur, n'est pas prise en charge. Avant d'activer Credential Guard, vous devez vous assurer que cette fonctionnalité est désactivée. Pour plus d'informations, consultez [Désactiver l'intégrité de la mémoire](#).

Types d'instances

Les types d'instances suivants prennent en charge Credential Guard, quelle que soit la taille : C5, C5d, C5n, C6i, C6id, C6in, M5, M5d, M5dn, M5n, M5zn, M6i, M6id, M6idn, M6in, R5, R5b, R5d, R5dn, R5n, R6i, R6id, R6idn, R6in.

Note

Bien que NitroTPM ait en commun certains types d'instance requis, le type d'instance doit être l'un des types ci-dessus pour prendre en charge Credential Guard.

Lancer une instance prise en charge

Vous pouvez utiliser la console Amazon EC2 ou AWS Command Line Interface (AWS CLI) pour lancer une instance compatible avec Credential Guard. Vous aurez besoin d'un ID AMI compatible pour lancer votre instance, qui est unique pour chaque Région AWS.

Tip

Vous pouvez utiliser le lien suivant pour découvrir et lancer des instances avec des AMI compatibles fournies par Amazon dans la console Amazon EC2 :

https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Amazon EC2 console

Pour lancer une instance à l'aide de la console Amazon EC2

Suivez les étapes pour [lancer une instance](#), en spécifiant un type d'instance pris en charge et une AMI Windows préconfigurée.

AWS CLI

Pour lancer une instance à l'aide du AWS CLI

Utilisez la commande [run-instances](#) pour lancer une instance à l'aide d'un type d'instance pris en charge et d'une AMI Windows préconfigurée.

```
aws ec2 run-instances \  
  --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-  
English-Full-Base \  
  --instance-type c6i.large \  
  --region us-east-1 \  
  --subnet-id subnet-id \  
  --key-name key-name
```

PowerShell

Pour lancer une instance à l'aide du AWS Tools for PowerShell

Utilisez la commande [New-EC2Instance](#) pour lancer une instance à l'aide d'un type d'instance pris en charge et d'une AMI Windows préconfigurée.

```
New-EC2Instance \  
  -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-  
English-Full-Base \  
  -InstanceType c6i.large \  
  -Region us-east-1 \  
  -SubnetId subnet-id \  
  -KeyName key-name
```

Désactiver l'intégrité de la mémoire

Vous pouvez utiliser l'éditeur de stratégie de groupe local pour désactiver l'intégrité de la mémoire dans les scénarios pris en charge. Les instructions suivantes peuvent être appliquées pour chaque paramètre de configuration dans le cadre de la protection de l'intégrité du code basée sur la virtualisation :

- **Activé sans verrouillage** : modifiez le paramètre sur **Désactivé** pour désactiver l'intégrité de la mémoire.
- **Activé avec verrouillage UEFI** : l'intégrité de la mémoire a été activée avec le verrouillage UEFI. L'intégrité de la mémoire ne peut pas être désactivée une fois qu'elle a été activée avec le verrouillage UEFI. Nous vous recommandons de créer une nouvelle instance en désactivant l'intégrité de la mémoire et de résilier l'instance non prise en charge si elle n'est pas utilisée.

Pour désactiver l'intégrité de la mémoire à l'aide de l'éditeur de stratégie de groupe local

1. Connectez-vous à votre instance en tant que compte utilisateur disposant de privilèges d'administrateur à l'aide du protocole RDP (Remote Desktop Protocol). Pour plus d'informations, consultez [the section called "Connectez-vous à votre instance Windows à l'aide d'un client RDP"](#).
2. Ouvrez le menu Démarrer et recherchez **cmd** pour lancer une invite de commande.
3. Exécutez la commande suivante pour ouvrir l'éditeur de stratégie de groupe local : `gpedit.msc`
4. Dans l'éditeur de stratégie de groupe locale, choisissez Configuration de l'ordinateur, Modèles d'administration, Système, Device Guard.
5. Sélectionnez Activer la sécurité basée sur la virtualisation, puis sélectionnez Modifier le paramètre de stratégie.
6. Ouvrez la liste déroulante des paramètres de la protection de l'intégrité du code basée sur la virtualisation, choisissez Désactivé, puis sélectionnez Appliquer.
7. Redémarrez l'instance pour appliquer les modifications.

Activez Credential Guard

Après avoir lancé une instance Windows avec un type d'instance pris en charge et une AMI compatible, et confirmé que l'intégrité de cette mémoire est désactivée, vous pouvez activer Credential Guard.

Important

Des privilèges d'administrateur sont nécessaires pour exécuter les étapes suivantes afin d'activer Credential Guard.

Pour activer Credential Guard

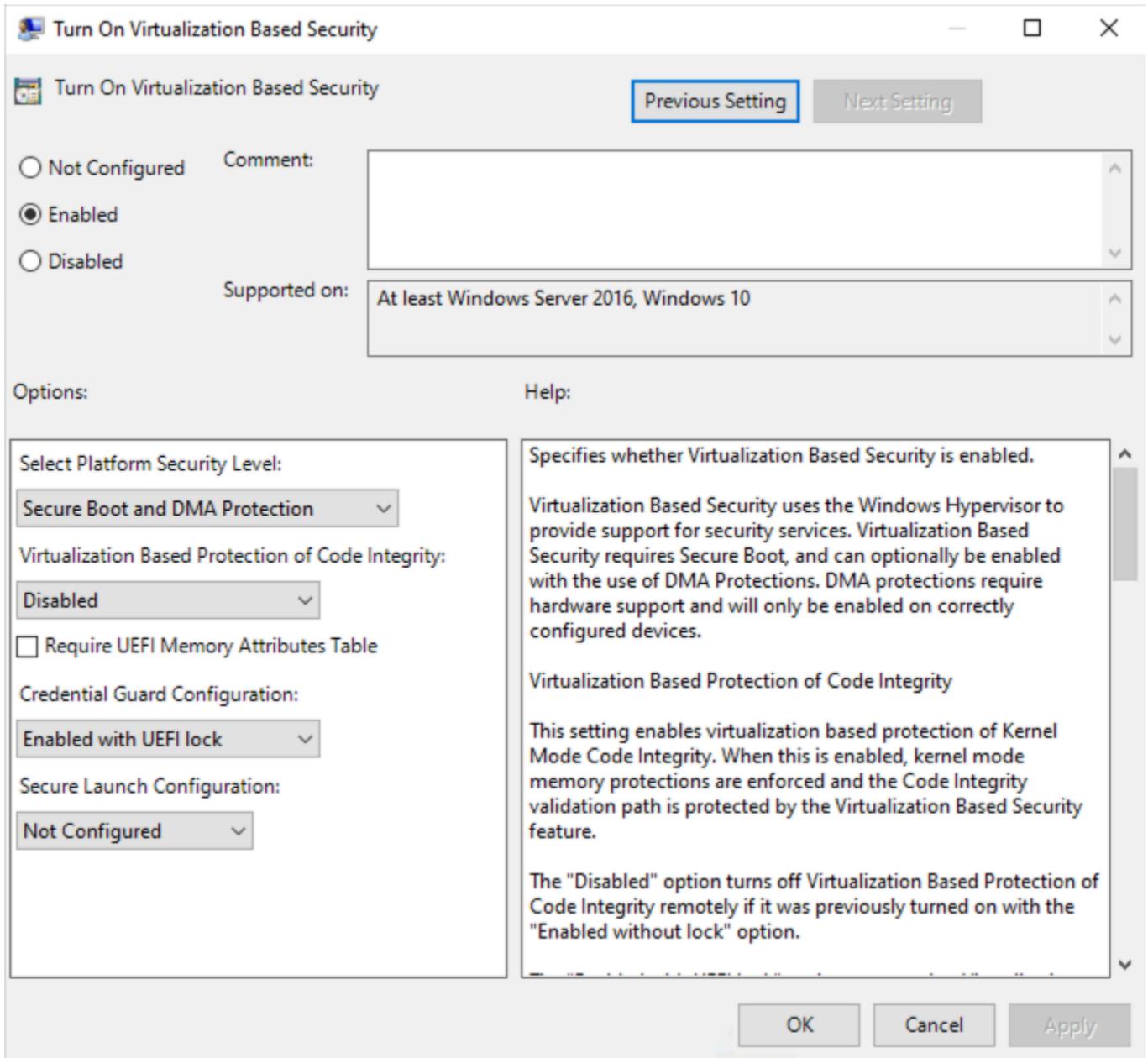
1. Connectez-vous à votre instance en tant que compte utilisateur disposant de privilèges d'administrateur à l'aide du protocole RDP (Remote Desktop Protocol). Pour plus d'informations, consultez [the section called "Connectez-vous à votre instance Windows à l'aide d'un client RDP"](#).
2. Ouvrez le menu Démarrer et recherchez **cmd** pour lancer une invite de commande.
3. Exécutez la commande suivante pour ouvrir l'éditeur de stratégie de groupe local : `gpedit.msc`
4. Dans l'éditeur de stratégie de groupe locale, choisissez Configuration de l'ordinateur, Modèles d'administration, Système, Device Guard.

5. Sélectionnez Activer la sécurité basée sur la virtualisation, puis sélectionnez Modifier le paramètre de stratégie.
6. Choisissez Activé dans le menu Activer la sécurité basée sur la virtualisation.
7. Pour Sélectionner le niveau de sécurité de la plateforme, choisissez Démarrage sécurisé et Protection DMA.
8. Pour la configuration de Credential Guard, choisissez Activé avec verrouillage UEFI.

 Note

Les autres paramètres de stratégie ne sont pas nécessaires pour activer Credential Guard et peuvent être laissés comme Non configurés.

L'image suivante affiche les paramètres VBS configurés comme décrit précédemment :



9. Redémarrez l'instance pour appliquer les paramètres.

Vérifiez que Credential Guard est en cours d'exécution

Vous pouvez utiliser l'outil Microsoft System Information (Msinfo32.exe) pour vérifier que Credential Guard est en cours d'exécution.

⚠ Important

Vous devez d'abord redémarrer l'instance pour terminer l'application des paramètres de stratégie nécessaires à l'activation de Credential Guard.

Pour vérifier que Credential Guard est en cours d'exécution

1. Connectez-vous à votre instance à l'aide du protocole RDP (Remote Desktop Protocol). Pour plus d'informations, consultez [the section called "Connectez-vous à votre instance Windows à l'aide d'un client RDP"](#).
2. Dans la session RDP de votre instance, ouvrez le menu Démarrer et recherchez **cmd** pour lancer une invite de commande.
3. Ouvrez System Information en exécutant la commande suivante : `msinfo32.exe`
4. L'outil Microsoft System Information répertorie les détails de la configuration VBS. À côté de Services de sécurité basés sur la virtualisation, vérifiez que Credential Guard apparaît comme étant en cours d'exécution.

L'image suivante montre que VBS est en cours d'exécution comme décrit précédemment :

Virtualization-based security	Running
Virtualization-based security Required Security Properties	Base Virtualization Support, Secure Boot, DMA Protection
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonly, Mode Based Execution Control
Virtualization-based security Services Configured	Credential Guard
Virtualization-based security Services Running	Credential Guard

Options de stockage pour vos instances Amazon EC2

Amazon EC2 vous propose des options de stockage de easy-to-use données flexibles et économiques pour vos instances. Chaque option est une combinaison unique de performance et de durabilité. Ces options de stockage peuvent être utilisées seules ou associées pour satisfaire vos besoins.

[Amazon EBS](#)

Amazon EBS fournit des volumes de stockage par bloc que vous pouvez attacher à vos instances et les en détacher. Vous pouvez également attacher plusieurs volumes EBS à une instance. Un volume EBS est permanent indépendamment de la durée de son instance associée. Vous pouvez chiffrer vos volumes EBS. Pour conserver une copie de sauvegarde de vos données, vous pouvez créer des instantanés à partir de vos volumes EBS. Les instantanés sont stockés dans Amazon S3. Vous pouvez créer un volume EBS à partir d'un instantané.

[Stockage d'instances](#)

Le stockage d'instances fournit un stockage temporaire de niveau bloc pour les instances. Le nombre, la taille et le type des volumes de stockage d'instances sont déterminés par le type et la taille des instances. Les données sur un volume de stockage d'instances persistent uniquement pendant la vie de l'instance associée. Si vous arrêtez, mettez en veille prolongée ou résiliez une instance, toutes les données sur les volumes de stockage d'instances sont perdues.

[Amazon EFS](#)(Instances Linux uniquement)

Amazon EFS offre un stockage de fichiers scalable, destiné à être utilisé avec Amazon EC2. Vous pouvez créer un système de fichiers EFS et configurer vos instances afin de l'installer. Vous pouvez utiliser un système de fichiers EFS comme source de données commune aux charges de travail et applications exécutées sur plusieurs instances.

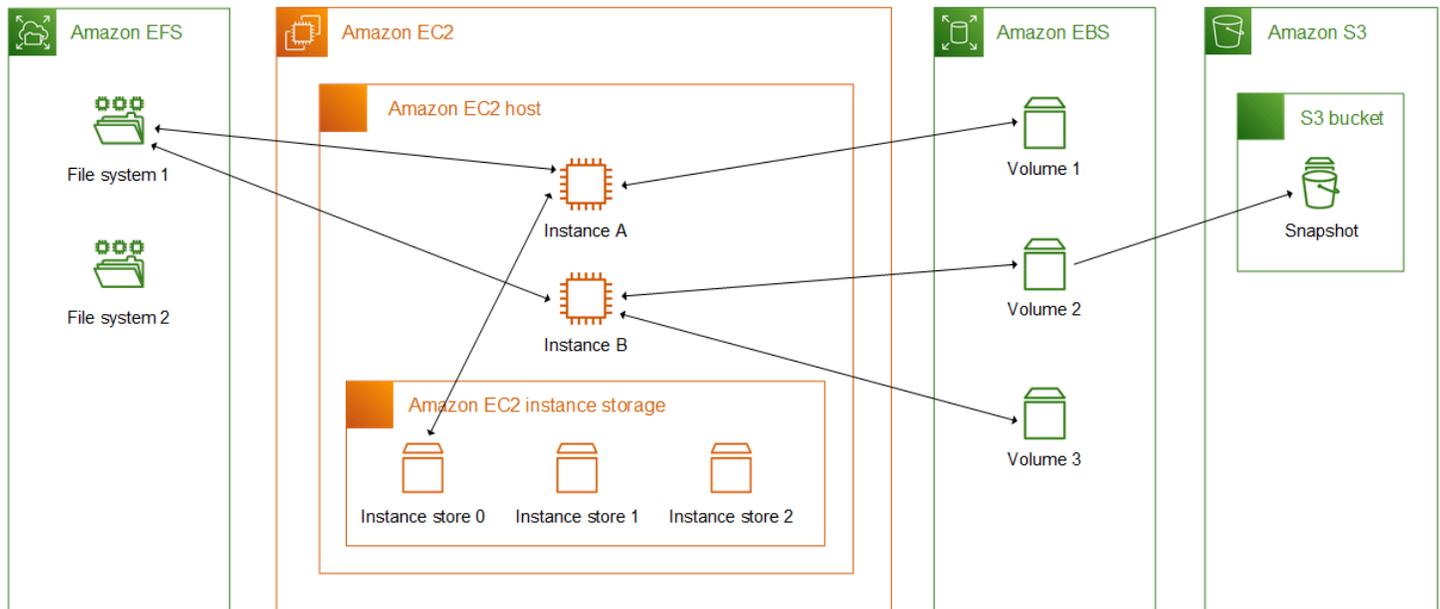
[Amazon S3](#)

Amazon S3 fournit un accès à une infrastructure de stockage de données fiable et économique. Cet outil est conçu pour faciliter l'accès aux ressources informatiques à l'échelle du Web en vous permettant de stocker et de récupérer à tout moment n'importe quelle quantité de données, depuis Amazon EC2, ou depuis n'importe quel emplacement sur le Web. Par exemple, vous pouvez utiliser Amazon S3 pour stocker des copies de sauvegarde de vos données et applications. Amazon EC2 utilise Amazon S3 pour stocker des instantanés EBS et des AMI basées sur le stockage d'instances.

Amazon FSx

Avec Amazon FSx, vous pouvez lancer, exécuter et mettre à l'échelle des systèmes de fichiers riches en fonctionnalités et haute performance dans le cloud. Amazon FSx est un service entièrement géré qui prend en charge un large éventail de charges de travail. Vous pouvez choisir entre ces systèmes de fichiers largement utilisés : Lustre, NetApp ONTAP, OpenZFS et Windows File Server.

L'illustration suivante représente la relation entre ces options de stockage et votre instance.



Tarification du stockage

Ouvrez [AWS Tarification](#), faites défiler la page jusqu'à Tarification AWS des produits et sélectionnez Stockage. Choisissez le produit de stockage pour ouvrir sa page de tarification.

Utiliser Amazon EBS avec Amazon EC2

Amazon Elastic Block Store (Amazon EBS) fournit des ressources de stockage par blocs évolutives et performantes qui peuvent être utilisées avec les instances Amazon Elastic Compute Cloud (Amazon EC2). Avec Amazon EBS, vous pouvez créer et gérer les ressources de stockage par blocs suivantes :

- Volumes Amazon EBS : il s'agit de volumes de stockage que vous attachez aux instances Amazon EC2. Une fois que vous avez attaché un volume à une instance, vous pouvez l'utiliser de la même

manière que vous utiliseriez le stockage par blocs. L'instance peut interagir avec le volume comme elle le ferait avec un lecteur local.

- Instantanés Amazon EBS : il s'agit de point-in-time sauvegardes de volumes Amazon EBS qui sont conservées indépendamment du volume lui-même. Vous pouvez créer des instantanés pour sauvegarder les données de vos volumes Amazon EBS. Vous pouvez ensuite restaurer de nouveaux volumes à partir de ces instantanés à tout moment.

Vous pouvez créer et associer des volumes Amazon EBS à une instance lors du lancement, et vous pouvez créer et attacher des volumes EBS à une instance à tout moment après le lancement. Et vous pouvez créer des instantanés à partir d'un volume à tout moment après sa création.

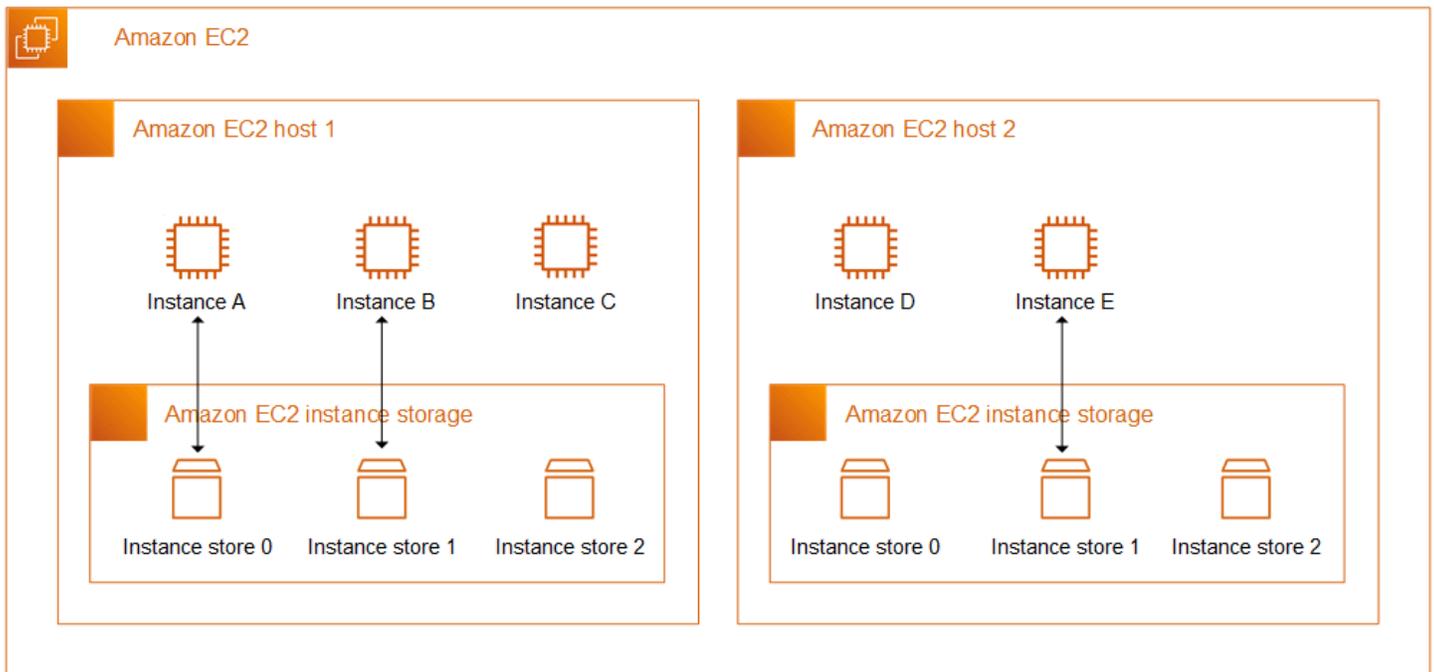
Pour plus d'informations sur l'utilisation des volumes et des instantanés, consultez le guide de [l'utilisateur Amazon EBS](#).

Stockage d'instances Amazon EC2

Un stockage d'instances fournit un stockage temporaire de niveau bloc pour votre instance. Le stockage réside sur les disques physiquement attachés à l'ordinateur hôte. Le stockage d'instances est particulièrement adapté pour le stockage temporaire d'informations qui changent fréquemment, telles que les tampons, les caches, les données de travail et autres contenus temporaires. Il peut également être utilisé pour stocker des données temporaires que vous répliquez sur une flotte d'instances, comme un groupe à charge équilibrée de serveurs Web.

Un stockage d'instances se compose d'un ou de plusieurs stockages d'instance exposés comme périphériques de stockage en mode bloc. La taille d'un stockage d'instances ainsi que le nombre de périphériques disponibles varient en fonction du type et de la taille des instances. Pour plus d'informations, consultez [Volumes de stockage d'instances](#).

Les périphériques virtuels des volumes de stockage d'instances sont `ephemeral[0-23]`. Les types d'instance qui prennent en charge un seul volume de stockage d'instances ont `ephemeral0`. Les types d'instances qui prennent en charge au moins deux volumes de stockage d'instances ont `ephemeral0`, `ephemeral1` et ainsi de suite.



Tarification du stockage d'instances

Les volumes de stockage d'instances sont inclus dans le coût d'utilisation de l'instance.

Table des matières

- [Volume du stockage d'instances et durée de vie des données](#)
- [Volumes de stockage d'instances](#)
- [Ajouter des volumes de stockage d'instance à votre instance EC2](#)
- [Volumes de stockage d'instance SSD](#)
- [Volumes d'échange de stockage d'instance pour les instances Linux](#)
- [Optimisation des performances du disque pour les volumes de stockage d'instance sur les instances Linux](#)

Volume du stockage d'instances et durée de vie des données

Le nombre, la taille et le type des volumes de stockage d'instances sont déterminés par le type et la taille des instances. Pour plus d'informations, consultez [Volumes de stockage d'instances](#).

Les volumes de stockage d'instances sont attachés uniquement au lancement de l'instance. Vous ne pouvez pas attacher des volumes de stockage d'instances après le lancement. Vous ne pouvez pas détacher un volume de stockage d'instances à partir d'une instance et l'attacher à une autre instance.

Un volume de stockage d'instances n'existe que pendant la durée de vie de l'instance à laquelle il est attaché. Vous ne pouvez pas configurer un volume de stockage d'instances pour qu'il persiste au-delà de la durée de vie de son instance associée.

Les données stockées sur un volume de stockage d'instances persistent même si l'instance est redémarrée. Toutefois, les données ne persistent pas si l'instance est arrêtée, mise en veille prolongée ou résiliée. Lorsque l'instance est arrêtée, mise en veille prolongée ou résiliée, chaque bloc du stockage d'instances est effacé de manière cryptographique.

Par conséquent, ne vous fiez pas au stockage d'instances pour les données précieuses et à long terme. Si vous devez conserver les données stockées sur un volume de stockage d'instances au-delà de la durée de vie de l'instance, vous devez copier manuellement ces données vers un stockage plus persistant, tel qu'un volume Amazon EBS, un compartiment Amazon S3 ou un système de fichiers Amazon EFS.

Certains événements peuvent empêcher la persistance de vos données pendant toute la durée de vie de l'instance. Le tableau suivant indique si les données relatives aux volumes de stockage d'instances sont persistées lors d'événements spécifiques, tant pour les instances virtualisées que pour les instances de matériel nu.

Événement	Qu'arrive-t-il à vos données ?
Événements du cycle de vie de l'instance initiés par l'utilisateur	
L'instance est redémarrée	Les données persistent
L'instance est arrêtée	Les données ne persistent pas
L'instance est mise en veille prolongée	Les données ne persistent pas
L'instance est terminée	Les données ne persistent pas
Le type d'instance est modifié	Les données ne persistent pas *
Une AMI basée sur EBS est créée à partir de l'instance	Les données ne sont pas conservées dans l'AMI créée**
Une AMI basée sur une instance store-backed est créée à partir de l'instance (instances Linux)	Les données sont conservées dans le bundle AMI chargé sur Amazon S3 ***

Événement	Qu'arrive-t-il à vos données ?
Événements du système d'exploitation initiés par l'utilisateur	
Un arrêt est lancé	Les données ne persistent pas †
Un redémarrage est lancé	Les données persistent
AWS événements programmés	
Arrêt de l'instance	Les données ne persistent pas
Redémarrage de l'instance	Les données persistent
Redémarrage du système	Les données persistent
Retrait d'instance	Les données ne persistent pas
Événements non planifiés	
Restauration automatique simplifiée	Les données ne persistent pas
CloudWatch restauration basée sur l'action	Les données ne persistent pas
Le disque sous-jacent tombe en panne	Les données présentes sur le disque défaillant ne sont pas conservées
Panne de courant	Les données sont conservées au redémarrage

* Si le nouveau type d'instance prend en charge le stockage d'instances, l'instance obtient le nombre de volumes de stockage d'instances pris en charge par le nouveau type d'instance, mais les données ne sont pas transférées vers la nouvelle instance. Si le nouveau type d'instance ne prend pas en charge le stockage d'instances, l'instance n'obtient pas les volumes de stockage d'instances.

** Les données ne sont pas incluses dans l'AMI basée sur EBS ni dans les volumes de stockage d'instances attachés aux instances lancées depuis cette AMI.

*** Les données sont incluses dans la création d'une offre groupée AMI qui est chargée dans Amazon S3. Lorsque vous lancez une instance à partir de cette AMI, l'instance obtient les volumes de stockage d'instances regroupés dans l'AMI avec les données qu'ils contenaient au moment de la création de l'AMI.

† La protection contre la résiliation et l'arrêt ne protègent pas les instances contre les arrêts ou les résiliations d'instances à la suite d'arrêts initiés via le système d'exploitation de l'instance. Les données stockées sur les volumes de stockage d'instances ne persistent pas lors des événements d'arrêt ni de résiliation d'instance.

Volumes de stockage d'instances

Le nombre, la taille et le type des volumes de stockage d'instances sont déterminés par le type et la taille des instances. Certains types d'instances, tels que M6, C6 et R6, ne prennent pas en charge les volumes de stockage d'instances, tandis que d'autres types d'instances, tels que M5d, C6gd et R6gd, prennent en charge les volumes de stockage d'instances. Vous ne pouvez pas attacher à une instance plus de volumes de stockage d'instances que ne le permet son type d'instance. Pour les types d'instances qui prennent en charge les volumes de stockage d'instances, le nombre et la taille des volumes de stockage d'instances varient en fonction de la taille de l'instance. Par exemple, `m5d.large` prend en charge 1 volume de stockage d'instances de 75 Go, tandis que `m5d.24xlarge` prend en charge 4 volumes de stockage d'instances de 900 Go.

Pour les types d'instances dotés de volumes de stockage d'instances NVMe, tous les volumes de stockage d'instances pris en charge sont automatiquement attachés à l'instance au lancement. Pour les types d'instance dotés de volumes de stockage d'instance non NVMe, tels que C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 et X1e, vous devez spécifier manuellement les mappages de périphériques de bloc pour les volumes de stockage d'instance que vous souhaitez associer au lancement. Ensuite, une fois l'instance lancée, vous devez [formater et monter les volumes de stockage d'instances attachés](#) avant de pouvoir les utiliser. Vous ne pouvez pas attacher un volume de stockage d'instances après avoir lancé l'instance.

Certains types d'instances utilisent des disques SSD NVMe ou basés sur SATA, tandis que d'autres utilisent des disques HDD basés sur SATA. Les disques SSD offrent une performance d'E/S aléatoires élevée, mais il n'est pas nécessaire que les données persistent lorsque l'instance est résiliée ou que vous pouvez tirer parti des architectures tolérantes aux pannes. Pour plus d'informations, consultez [Volumes de stockage d'instance SSD](#).

Les données sur les volumes de stockage d'instance NVMe et sur certains volumes de stockage d'instance HDD sont chiffrées au repos. Pour plus d'informations, consultez [Protection des données dans Amazon EC2](#).

Volumes de stockage d'instances disponibles

Le guide des types d'instances Amazon EC2 fournit des informations sur la quantité, la taille, le type et les optimisations des performances des volumes de stockage d'instance disponibles pour chaque type d'instance pris en charge. Pour plus d'informations, consultez les ressources suivantes :

- [Spécifications du magasin d'instances — Usage général](#)
- [Spécifications du magasin d'instances — Optimisé pour le calcul](#)
- [Spécifications du magasin d'instances — Mémoire optimisée](#)
- [Spécifications du magasin d'instances — Stockage optimisé](#)
- [Spécifications du magasin d'instances — Calcul accéléré](#)
- [Spécifications du magasin d'instances — Calcul à hautes performances](#)
- [Spécifications du magasin d'instances — Génération précédente](#)

Pour récupérer les informations sur le volume de stockage de l'instance à l'aide du AWS CLI

Vous pouvez utiliser la AWS CLI commande [describe-instance-types](#) pour afficher des informations sur un type d'instance, telles que ses volumes de stockage d'instance. L'exemple suivant affiche la taille totale du stockage d'instance de toutes les instances R5 avec volumes de stockage d'instance.

```
aws ec2 describe-instance-types \
  --filters "Name=instance-type,Values=r5*" "Name=instance-storage-
supported,Values=true" \
  --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
  --output table
```

Exemple de sortie

```
-----
| DescribeInstanceTypes |
+-----+-----+
| r5ad.24xlarge | 3600 |
| r5ad.12xlarge | 1800 |
| r5dn.8xlarge  | 1200 |
| r5ad.8xlarge  | 1200 |
| r5ad.large    | 75   |
| r5d.4xlarge   | 600  |
| . . .        |      |
```

```
| r5dn.2xlarge | 300 |  
| r5d.12xlarge | 1800 |  
+-----+-----+
```

L'exemple suivant affiche les détails complets du stockage d'instance correspondant au type d'instance spécifié.

```
aws ec2 describe-instance-types \  
  --filters "Name=instance-type,Values=r5d.4xlarge" \  
  --query "InstanceTypes[].InstanceStorageInfo"
```

L'exemple de sortie montre que ce type d'instance possède deux volumes SSD NVMe de 300 Go, pour un total de 600 Go de stockage d'instance.

```
[  
  {  
    "TotalSizeInGB": 600,  
    "Disks": [  
      {  
        "SizeInGB": 300,  
        "Count": 2,  
        "Type": "ssd"  
      }  
    ],  
    "NvmeSupport": "required"  
  }  
]
```

Ajouter des volumes de stockage d'instance à votre instance EC2

Pour les types d'instances dotés de volumes de stockage d'instances NVMe, tous les volumes de stockage d'instances pris en charge sont automatiquement attachés à l'instance au lancement. Ils sont automatiquement énumérés et un nom de périphérique leur est automatiquement attribué au lancement de l'instance.

Pour les types d'instance dotés de volumes de stockage d'instance non NVME, tels que C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 et X1e, vous devez spécifier manuellement les mappages de périphériques de bloc pour les volumes de stockage d'instance que vous souhaitez associer au lancement. Les mappages de périphériques de stockage en mode bloc peuvent être spécifiés dans la requête de lancement d'instance ou dans l'AMI utilisée pour lancer l'instance. Le mappage de

périphérique de stockage en mode bloc inclut un nom de périphérique et le volume sur lequel il est mappé. Pour plus d'informations, consultez [Mappages de périphériques de stockage en mode bloc](#).

Important

Vous ne pouvez attacher les volumes de stockage d'instances à une instance que lors de son lancement. Vous ne pouvez pas attacher des volumes de stockage d'instance à une instance après l'avoir lancée.

Après le lancement d'une instance, vous devez vous assurer que les volumes de stockage d'instance de votre instance sont formatés et montés avant que vous ne puissiez les utiliser. Le volume racine d'une instance basée sur le stockage d'instance est monté automatiquement.

À prendre en compte pour les volumes racines

Un mappage de périphérique de stockage en mode bloc spécifie toujours le volume racine de l'instance. Le volume racine est toujours monté automatiquement.

Instances Linux : le volume racine est soit un volume Amazon EBS, soit un volume de stockage d'instance. Dans le cas des instances ayant un volume de stockage d'instance pour le volume racine, la taille de ce volume varie en fonction de l'AMI, mais la taille maximale est de 10 Go. Pour plus d'informations, consultez [Stockage pour le périphérique racine](#).

Instances Windows : le volume racine doit être un volume Amazon EBS. Le stockage d'instance n'est pas pris en charge pour le volume racine.

Table des matières

- [Ajouter des volumes de stockage d'instance à une AMI](#)
- [Ajouter des volumes de stockage d'instances non NVMe à une instance](#)
- [Rendre disponibles les volumes de stockage d'instance sur votre instance](#)

Ajouter des volumes de stockage d'instance à une AMI

Vous pouvez créer une AMI avec un mappage de périphérique de stockage en mode bloc incluant des volumes de stockage d'instance.

Si vous lancez une instance qui prend en charge les volumes de stockage d'instances non NVMe à l'aide d'une AMI qui spécifie les mappages de périphérique de stockage en mode bloc de volume

de stockage d'instances, l'instance inclut ces volumes de stockage d'instances. Si le nombre de volumes de stockage d'instances dans les mappages de périphérique de stockage en mode bloc dépasse le nombre de volumes de stockage d'instances disponibles pour l'instance, les mappages de périphérique de stockage en mode bloc de volume de stockage d'instances supplémentaires sont ignorés.

Si vous lancez une instance qui prend en charge les volumes de stockage d'instances NVMe à l'aide d'une AMI qui spécifie les volumes de stockage d'instances dans son mappage de périphérique de stockage en mode bloc, les mappages de périphérique de stockage en mode bloc de volume de stockage d'instances sont ignorés. Les instances qui prennent en charge les volumes de stockage d'instances NVMe ont tous leurs volumes de stockage d'instances pris en charge, quels que soient les mappages de périphérique de stockage en mode bloc spécifiés dans la requête de lancement de l'instance et dans l'AMI.

Considérations

- Pour les instances M3, spécifiez les volumes de stockage d'instances dans le mappage de périphérique de stockage en mode bloc de l'instance, pas dans l'AMI. Amazon EC2 peut ignorer les volumes de stockage d'instances dans le mappage de périphérique de stockage en mode bloc de l'AMI.
- Lors du lancement d'une instance, vous pouvez omettre les volumes de stockage d'instances non NVMe spécifiés dans le mappage d'appareils de stockage en mode bloc de l'AMI et ajouter de nouveaux volumes de stockage d'instances.

New console

Pour ajouter des volumes de stockage d'instance à une AMI basée sur des volumes Amazon EBS à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances, puis choisissez l'instance.
3. Choisissez Actions, Image and templates (Image et modèles), Create image (Créer une image).
4. Sur la page Create Image (Créer une image), saisissez un nom et une description significatifs pour votre image.
5. Pour chaque volume de stockage d'instance à ajouter, sélectionnez Add volume (Ajouter un volume), puis dans Type de volume, sélectionnez un volume de stockage d'instance, et

dans Device (Périphérique), sélectionnez un nom de périphérique. (Pour plus d'informations, consultez [Noms des appareils sur les instances Amazon EC2](#).) Le nombre de volumes de stockage d'instance disponibles dépend du type d'instance. Pour les instances avec volumes de stockage d'instance NVMe, le mappage de périphérique de ces volumes dépend de l'ordre dans lequel le système d'exploitation énumère les volumes.

6. Choisissez Create image (Créer une image).

AWS CLI

Pour ajouter des volumes de stockage d'instance à une AMI à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [create-image](#) ou [register-image](#) (AWS CLI)
- [New-EC2Image](#) et [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

Ajouter des volumes de stockage d'instances non NVMe à une instance

Lorsque vous lancez une instance qui prend en charge les volumes de stockage d'instances non NVMe, vous devez spécifier les mappages de périphérique de stockage en mode bloc des volumes de stockage d'instances à attacher. Les mappages de périphérique de stockage en mode bloc doivent être spécifiés dans la requête de lancement de l'instance ou dans l'AMI utilisée pour lancer l'instance.

Si l'AMI inclut des mappages de périphérique de stockage en mode bloc pour les volumes de stockage d'instances, vous n'avez pas besoin de spécifier de mappages de périphérique de stockage en mode bloc dans la requête de lancement de l'instance, sauf si vous avez besoin de volumes de stockage d'instances supérieurs à ceux inclus dans l'AMI.

Si l'AMI n'inclut pas de mappages de périphérique de stockage en mode bloc pour les volumes de stockage d'instances, vous devez spécifier les mappages de périphérique de stockage en mode bloc dans la requête de lancement de l'instance.

Considérations

- Pour les instances M3, il se peut que vous receviez les volumes de stockage d'instance, même si vous ne les spécifiez pas dans le mappage de périphérique de stockage en mode bloc de l'instance.

Pour spécifier des mappages de périphérique de stockage en mode bloc dans la requête de lancement de l'instance, utilisez l'une des méthodes suivantes.

Amazon EC2 console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le tableau de bord, choisissez Lancer une instance.
3. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez l'AMI à utiliser.
4. Dans Configurer le stockage, la section Volumes de stockage d'instances répertorie les volumes de stockage d'instances qui peuvent être attachés à l'instance. Le nombre de volumes de stockage d'instance disponibles dépend du type d'instance.
5. Pour chaque volume de stockage d'instances à attacher, dans Nom du périphérique, sélectionnez le nom du périphérique à utiliser.
6. Configurez les paramètres d'instance restants selon les besoins, puis cliquez sur Lancer l'instance.

Command line

Vous pouvez utiliser l'une des commandes suivantes avec l'option correspondante.

- `--block-device-mappings` avec [run-instances](#) (AWS CLI)
- `-BlockDeviceMapping` avec [New-EC2Instance](#) (AWS Tools for Windows PowerShell)

Rendre disponibles les volumes de stockage d'instance sur votre instance

Après avoir lancé une instance avec des volumes de stockage d'instances associés, vous devez monter les volumes avant de pouvoir y accéder.

Note

La plupart des volumes de stockage d'instance sont préformatés avec le système de fichiers ext3. Les volumes de stockage d'instance SSD prenant en charge l'instruction TRIM ne sont pas préformatés avec un système de fichiers. Cependant, vous pouvez formater les volumes avec le système de fichiers de votre choix après avoir lancé votre instance. Pour plus d'informations, consultez [Prise en charge de TRIM sur les volumes de stockage d'instance](#).

Pour les instances Windows, nous reformatons les volumes de stockage d'instances avec le système de fichiers NTFS.

Instances Linux

Vous pouvez afficher et monter les volumes de stockage de l'instance comme décrit dans la procédure suivante.

Pour rendre disponible un volume de stockage d'instance sur Linux

1. Connectez-vous à l'instance à l'aide d'un client SSH. Pour plus d'informations, consultez [Connectez-vous à votre instance Linux](#).
2. Utilisez la commande `df -h` pour afficher les volumes qui sont formatés et montés.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G  72K  3.8G   1% /dev
tmpfs           3.8G   0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Utilisez la commande `lsblk` pour afficher les volumes qui ont été mappés au lancement, mais ne sont ni formatés ni montés.

```
$ lsblk
NAME            MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1         259:1   0    8G  0 disk
##nvme0n1p1    259:2   0    8G  0 part /
##nvme0n1p128 259:3   0    1M  0 part
nvme1n1         259:0   0 69.9G  0 disk
```

4. Pour formater et monter un volume de stockage d'instance qui a seulement été mappé, procédez comme suit :
 - a. Créez un système de fichiers sur le périphérique avec la commande `mkfs`.

```
$ sudo mkfs -t xfs /dev/nvme1n1
```

- b. Créez un répertoire sur lequel monter le périphérique avec la commande `mkdir`.

```
$ sudo mkdir /data
```

- c. Montez le périphérique sur le répertoire nouvellement créé à l'aide de la commande mount.

```
$ sudo mount /dev/nvme1n1 /data
```

instances Windows

Vous pouvez également afficher les volumes de stockage des instances à l'aide de Windows Disk Management. Pour plus d'informations, consultez [Référencer les disques à l'aide de la gestion des disques](#).

Pour monter manuellement un volume de stockage d'instance

1. Choisissez Start (Démarrer), entrez Computer Management (Gestion de l'ordinateur), puis appuyez sur Entrée.
2. Dans le panneau de gauche, choisissez Disk Management (Gestion des disques).
3. Si vous êtes invité à initialiser le volume, choisissez le volume à initialiser, sélectionnez le type de partition requis en fonction de votre cas d'utilisation, puis choisissez OK.
4. Dans la liste des volumes, cliquez avec le bouton droit sur le volume à monter, puis choisissez New Simple Volume (Nouveau volume simple).
5. Dans l'assistant, choisissez Next (Suivant).
6. Dans l'écran de spécification de la taille du volume, choisissez Next (Suivant) pour utiliser la taille de volume maximale. Vous pouvez également choisir une taille de volume comprise entre l'espace disque minimal et maximal.
7. Dans l'écran d'affectation d'une lettre de lecteur ou d'un chemin, effectuez l'une des opérations suivantes et choisissez Next (Suivant).
 - Pour monter le volume avec une lettre de lecteur, choisissez Assign the following drive letter (Affecter la lettre de lecteur suivante) puis choisissez la lettre de lecteur à utiliser.
 - Pour monter le volume en tant que dossier, choisissez Mount in the following empty NTFS folder (Monter dans le dossier NTFS vide suivant), puis choisissez Browse (Parcourir) pour créer ou sélectionner le dossier à utiliser.
 - Pour monter le volume sans lettre de lecteur ou chemin d'accès, choisissez Do not assign a drive letter or drive path (Ne pas affecter de lettre ou de chemin d'accès de lecteur).

8. Dans l'écran de formatage de partition, indiquez si le volume doit être formaté ou non. Si vous choisissez de formater le volume, choisissez le système de fichiers requis et la taille de l'unité, puis spécifiez un libellé de volume.
9. Choisissez Next (Suivant), Finish (Terminer).

Pour obtenir des instructions sur le montage automatique d'un volume attaché après le redémarrage, consultez la section [Montage automatique d'un volume attaché après le redémarrage](#) dans le guide de l'utilisateur Amazon EBS.

Volumes de stockage d'instance SSD

Comme pour tout autre volume de stockage d'instance, vous devez mapper les volumes de stockage d'instance SSD de votre instance lorsque cette dernière est lancée. Les données d'un volume d'instance SSD ne persistent que pendant la vie de son instance associée. Pour plus d'informations, consultez [Ajouter des volumes de stockage d'instance à votre instance EC2](#).

Volumes SSD NVMe

Certaines instances offrent des volumes de stockage d'instance SSD NVMe (Non-Volatile Memory Express). Pour plus d'informations sur le type de volume de stockage d'instance pris en charge par chaque type d'instance, consultez [Volumes de stockage d'instances](#).

Les données sur le stockage d'instance NVMe sont chiffrées à l'aide d'un chiffrement par blocs XTS-AES-256 implémenté dans un module matériel sur l'instance. Les clés de chiffrement sont générées à l'aide du module matériel et sont uniques pour chaque périphérique de stockage d'instance NVMe. Toutes les clés de chiffrement sont détruites lorsque l'instance est arrêtée ou résiliée et ne peuvent pas être récupérées. Vous ne pouvez pas désactiver le chiffrement et vous ne pouvez pas fournir votre propre clé de chiffrement.

Instances Linux

Pour accéder aux volumes NVMe, les [pilotes NVMe](#) doivent être installés. Les AMI suivantes satisfont cette exigence :

- AL2023
- Amazon Linux 2
- Amazon Linux AMI 2018.03 et version ultérieure
- Ubuntu 14.04 ou une version ultérieure avec noyau `linux-aws`

Note

AWS Les types d'instances basés sur Graviton nécessitent Ubuntu 18.04 ou version ultérieure avec noyau `linux-aws`

- Red Hat Enterprise Linux 7.4 ou une version ultérieure
- SUSE Linux Enterprise Server 12 SP2 ou une version ultérieure
- CentOS 7.4.1708 ou une version ultérieure
- FreeBSD 11.1 ou une version ultérieure
- Debian GNU/Linux 9 ou version ultérieure

- Bottlerocket

Après avoir connecté votre instance, vous pouvez répertorier les périphériques NVMe à l'aide de la commande `lspci`. Voici un exemple de sortie d'une instance `i3.xlarge`, qui prend en charge quatre périphériques NVMe.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Si vous utilisez un système d'exploitation pris en charge, mais que les périphériques NVMe ne sont pas visibles, vérifiez que le module NVMe est chargé à l'aide de la commande suivante.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

```
$ lsmod | grep nvme
```

```
nvme          48813  0
```

- Ubuntu 18

```
$ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
s/nvme/host/nvme-core.ko
kernel/drivers/nvme/host/nvme.ko
kernel/drivers/nvme/nvme_core.ko
```

Les volumes NVMe sont conformes à la spécification NVMe 1.0e. Vous pouvez utiliser les commandes NVMe avec vos volumes NVMe. Avec Amazon Linux, vous pouvez installer le package `nvme-cli` à partir du référentiel à l'aide de la commande `yum install`. Avec d'autres versions de Linux prises en charge, vous pouvez télécharger le package `nvme-cli` s'il n'est pas disponible dans l'image.

instances Windows

Les dernières AMI AWS Windows pour les systèmes d'exploitation suivants contiennent les pilotes AWS NVMe utilisés pour interagir avec les volumes de stockage d'instances SSD qui sont exposés sous forme de périphériques en mode bloc NVMe pour de meilleures performances :

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Après avoir connecté votre instance, vous pouvez vérifier que les volumes NVMe s'affichent dans le gestionnaire de disque. Dans la barre des tâches, ouvrez le menu contextuel (via un clic droit) du logo Windows et choisissez Gestion des disques.

Les AMI AWS Windows fournies par Amazon incluent le pilote AWS NVMe. Si vous n'utilisez pas les dernières AMI AWS Windows, vous pouvez [installer le pilote AWS NVMe actuel](#).

Volumes SSD non NVMe

Les instances suivantes prennent en charge les volumes de stockage d'instance qui utilisent des SSD autres que NVMe pour fournir des performances d'E/S aléatoires élevées : C3, I2, M3, R3 et X1.

Pour plus d'informations sur la prise en charge des volumes de stockage d'instance par chaque type d'instance, consultez [Volumes de stockage d'instances](#).

Performances d'E/S du volume de stockage d'instances basé sur un SSD

Au fur et à mesure que vous remplissez les volumes de stockage d'instances basés sur SSD pour votre instance, le nombre d'IOPS en écriture que vous pouvez obtenir diminue. Ceci est dû au travail supplémentaire que le contrôleur SSD doit effectuer pour trouver de l'espace disponible, réécrire les données existantes et effacer l'espace non utilisé pour le rendre réinscriptible. Ce processus de nettoyage de la mémoire se traduit par une amplification d'écriture interne sur le disque SSD, exprimée sous la forme du rapport des opérations d'écriture SSD sur les opérations d'écriture utilisateur. Cette diminution des performances est encore plus importante si les opérations d'écriture ne sont pas exprimées en multiples de 4 096 octets ou ne sont pas alignées sur une limite de 4 096 octets. Si vous écrivez une quantité d'octets plus faible ou des octets qui ne sont pas alignés, le contrôleur SSD doit lire les données environnantes et stocker le résultat dans un nouvel emplacement. Ce modèle se traduit par une forte augmentation de l'amplification d'écriture, une latence accrue et une diminution considérable des performances d'I/O.

Les contrôleurs SSD peuvent utiliser plusieurs stratégies pour réduire l'impact de l'amplification d'écriture. Une telle stratégie consiste à réserver un espace dans le stockage d'instance SSD afin que le contrôleur puisse gérer efficacement l'espace disponible pour les opérations d'écriture. Cette solution est appelée sur-provisionnement. Les volumes de stockage d'instance SSD fournis à une instance ne disposent d'aucun espace réservé au surprovisionnement. Pour réduire l'amplification en écriture, nous vous recommandons de laisser 10 % du volume non partitionné afin que le contrôleur SSD puisse l'utiliser pour le surprovisionnement. Cela diminue le stockage que vous pouvez utiliser, mais augmente les performances même si le disque est proche de sa capacité maximale.

Par exemple, pour les volumes de stockage compatibles TRIM, vous pouvez utiliser la commande TRIM pour avertir le contrôleur SSD chaque fois que vous n'avez plus besoin des données que vous avez écrites. Cela fournit au contrôleur plus d'espace disponible, ce qui peut réduire l'amplification d'écriture et augmenter les performances. Pour plus d'informations, consultez [Prise en charge de TRIM sur les volumes de stockage d'instance](#).

Prise en charge de TRIM sur les volumes de stockage d'instance

Certains types d'instance prennent en charge les volumes SSD avec TRIM. Pour plus d'informations, consultez [Volumes de stockage d'instances](#).

Note

(Instances Windows uniquement) Les instances exécutant Windows Server 2012 R2 prennent en charge le TRIM à partir de la version 7.3.0 du pilote AWS PV. Les instances exécutant des versions antérieures de Windows Server ne prennent pas en charge TRIM.

Les volumes de stockage d'instance qui prennent en charge TRIM sont intégralement soumis à l'instruction TRIM avant d'être alloués à votre instance. Comme ces volumes ne sont pas formatés avec un système de fichiers au lancement de l'instance, vous devez les formater avant qu'ils ne puissent être montés et utilisés. Pour un accès plus rapide à ces volumes, vous devez ignorer l'opération TRIM lorsque vous les formatez.

(Instances Windows) Pour désactiver temporairement le support TRIM lors du formatage initial, utilisez la `fsutil behavior set DisableDeleteNotify 1` commande. Une fois le formatage terminé, réactivez le support TRIM en utilisant `fsutil behavior set DisableDeleteNotify 0`.

Avec les volumes de stockage d'instance qui prennent en charge TRIM, vous pouvez utiliser la commande TRIM pour informer le contrôleur SSD du moment où vous n'avez plus besoin des données que vous avez écrites. Cela fournit au contrôleur plus d'espace disponible, ce qui peut réduire l'amplification d'écriture et augmenter les performances. Sur les instances Linux, utilisez la `fstrim` commande pour activer le TRIM périodique. Sur les instances Windows, utilisez la `fsutil behavior set DisableDeleteNotify 0` commande pour vous assurer que le support TRIM est activé pendant le fonctionnement normal.

Volumes d'échange de stockage d'instance pour les instances Linux

Note

Cette rubrique s'applique uniquement aux instances Linux.

L'espace d'échange de Linux peut être utilisé quand un système nécessite plus de mémoire que celle qui lui a été allouée physiquement. Quand l'espace d'échange est activé, les systèmes Linux peuvent échanger exceptionnellement les pages mémoire utilisées entre la mémoire physique et l'espace d'échange (partition dédiée ou fichier d'échange d'un système de fichiers existant) et libérer cet espace pour les pages mémoire qui nécessitent un accès à haute vitesse.

Note

L'utilisation de l'espace d'échange pour la pagination mémoire n'est pas aussi rapide ou efficace que celle de la RAM. Si votre charge de travail pagine régulièrement la mémoire dans l'espace d'échange, envisagez de migrer vers un type d'instance plus grand avec plus de RAM. Pour plus d'informations, consultez [Modifier le type d'instance](#).

Les types d'instance `c1.medium` et `m1.small` ont une quantité limitée de mémoire physique à utiliser et bénéficient d'un volume d'échange de 900 Mio au moment du lancement qui fait office de mémoire virtuelle pour les AMIs Linux. Même si le noyau Linux considère cet espace d'échange comme une partition du périphérique racine, il s'agit réellement d'un volume de stockage d'instance distinct, quel que soit votre type de périphérique racine.

Amazon Linux active et utilise automatiquement cet espace d'échange et l'utilisent, mais il se peut que votre AMI nécessite quelques étapes supplémentaires pour reconnaître et utiliser cet espace d'échange. Pour vérifier si votre instance utilise un espace d'échange, vous pouvez utiliser la commande `swapon -s`.

```
[ec2-user ~]$ swapon -s
```

Filename	Type	Size	Used	Priority
/dev/xvda3	partition	917500	0	-1

L'instance ci-dessus possède un volume d'échange de 900 Mio attaché et activé. Si vous ne voyez aucun volume d'échange apparaître avec cette commande, vous devez peut-être activer l'espace d'échange pour le périphérique. Vérifiez vos disques disponibles à l'aide de la commande `lsblk`.

```
[ec2-user ~]$ lsblk
```

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT
xvda1	202:1	0	8G	0	disk	/
xvda3	202:3	0	896M	0	disk	

Ici, le volume d'échange `xvda3` est accessible à l'instance, mais il n'est pas activé (notez que le champ `MOUNTPOINT` est vide). Vous pouvez activer le volume d'échange avec la commande `swapon`.

Note

Vous devez préfixer par `/dev/` le nom du périphérique affiché par `lsblk`. Votre périphérique peut avoir un nom différent, tel que `sda3`, `sde3` ou `xvde3`. Utilisez le nom de périphérique pour votre système dans la commande ci-après.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

L'espace d'échange apparaît désormais dans la sortie `lsblk` et `swapon -s`.

```
[ec2-user ~]$ lsblk
NAME MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1   0    8G  0 disk /
xvda3 202:3   0 896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type              Size      Used      Priority
/dev/xvda3                               partition         917500    0         -1
```

Vous devez aussi modifier votre fichier `/etc/fstab` de telle sorte que cet espace d'échange soit automatiquement activé à chaque démarrage système.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Ajoutez la ligne suivante à votre fichier `/etc/fstab` (à l'aide du nom du périphérique d'échange de votre système) :

```
/dev/xvda3    none    swap    sw    0    0
```

Pour utiliser un volume de stockage d'instance comme espace d'échange

Tout volume de stockage d'instance peut être utilisé comme espace d'échange. Par exemple, le type d'instance `m3.medium` inclut un volume de stockage d'instance SSD de 4 Go, qui convient à l'espace d'échange. Si votre volume de stockage d'instance est beaucoup plus grand (par exemple, 350 Go), vous pouvez envisager de partitionner le volume avec une partition d'échange plus petite de 4 à 8 Go, le reste étant affecté à un volume de données.

Note

Cette procédure s'applique uniquement aux types d'instance prenant en charge ce stockage d'instance. Pour obtenir la liste des types d'instances, consultez [Volumes de stockage d'instances](#).

1. Affichez les périphériques de stockage en mode bloc attachés à votre instance pour obtenir le nom de périphérique de votre volume de stockage d'instance.

```
[ec2-user ~]$ lsblk -p
NAME          MAJ:MIN RM  SIZE RO  TYPE MOUNTPOINT
/dev/xvdb     202:16   0    4G  0  disk /media/ephemeral0
/dev/xvda1    202:1    0    8G  0  disk /
```

Dans cet exemple, le volume de stockage d'instance est `/dev/xvdb`. Comme il s'agit d'une instance Amazon Linux, le volume de stockage d'instance est formaté et monté à `/media/ephemeral0` ; certains systèmes d'exploitation Linux n'opèrent pas ainsi automatiquement.

2. (Facultatif) Si votre volume de stockage d'instance est monté (il affiche un MOUNTPOINT dans la sortie de la commande `lsblk`), vous devez le démonter à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Configurez une zone d'échange Linux sur le périphérique avec la commande `mkswap`.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Activez le nouvel espace d'échange.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Vérifiez que le nouvel espace d'échange est en cours d'utilisation.

```
[ec2-user ~]$ swapon -s
Filename      Type  Size Used Priority
/dev/xvdb                    partition 4188668 0 -1
```

6. Modifiez votre fichier `/etc/fstab` de telle sorte que cet espace d'échange soit automatiquement activé à chaque démarrage système.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Si votre fichier `/etc/fstab` a une entrée pour `/dev/xvdb` (ou `/dev/sdb`), modifiez-la pour qu'elle corresponde à la ligne ci-dessous ; dans le cas contraire, ajoutez la ligne suivante à votre fichier `/etc/fstab` (à l'aide du nom de périphérique d'échange de votre système) :

```
/dev/xvdb    none    swap    sw    0    0
```

Important

Les données du volume de stockage d'instance sont perdues quand une instance est arrêtée ou mise en veille prolongée. Cela inclut également le formatage de l'espace d'échange du volume de stockage créé dans [Step 3](#). Si vous arrêtez et redémarrez une instance qui a été configurée pour utiliser un espace d'échange de stockage d'instance, vous devez répéter [Step 1](#) via [Step 5](#) sur le nouveau volume de stockage d'instance.

Optimisation des performances du disque pour les volumes de stockage d'instance sur les instances Linux

Note

Cette rubrique s'applique uniquement aux instances Linux.

En raison de la façon dont Amazon EC2 virtualise les disques, la première écriture sur tout emplacement de certains volumes de stockage d'instance s'effectue plus lentement que les écritures suivantes. Pour la plupart des applications, l'amortissement de ce coût sur la durée de vie de l'instance est acceptable. Cependant, si vous exigez des performances disque élevées, il est recommandé que vous initialisiez vos disques en écrivant une fois sur chaque emplacement disque avant l'utilisation en production.

Note

Certains types d'instance dotés de disques SSD et de la prise en charge de la commande TRIM offrent des performances maximales au lancement, sans initialisation. Pour plus d'informations sur le stockage d'instance pour chaque type d'instance, consultez [Volumes de stockage d'instances](#).

Si vous exigez une plus grande souplesse en termes de latence ou de débit, nous vous recommandons l'utilisation d'Amazon EBS.

Pour initialiser les volumes de stockage d'instance, utilisez les commandes dd suivantes, en fonction du stockage à initialiser (par exemple, /dev/sdb ou /dev/nvme1n1).

Note

Veillez bien à démonter le disque avant d'exécuter cette commande. L'initialisation peut durer longtemps (8 heures environ pour une grande instance supplémentaire).

Pour initialiser les volumes de stockage d'instance, utilisez les commandes suivantes sur les types d'instance m1.large, m1.xlarge, c1.xlarge, m2.xlarge, m2.2xlarge et m2.4xlarge :

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Pour initialiser simultanément tous les volumes de stockage d'instance, utilisez la commande suivante :

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

La configuration des disques d'un système RAID les initialise en écrivant sur chaque emplacement disque. Lors de la configuration d'un système RAID basé sur un logiciel, assurez-vous de modifier la vitesse de reconstruction minimale :

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Stockage de fichiers

Le stockage de fichiers dans le cloud est une méthode de stockage des données dans le cloud qui permet aux serveurs et aux applications d'accéder aux données via des systèmes de fichiers partagés. Cette compatibilité rend le stockage de fichiers dans le cloud idéal pour les charges de travail reposant sur des systèmes de fichiers partagés et offre une intégration simple sans modification de code.

Il existe de nombreuses solutions de stockage de fichiers, allant d'un serveur de fichiers à nœud unique sur une instance de calcul utilisant le stockage par blocs comme base, sans évolutivité ou peu de redondances pour protéger les données, à une solution en do-it-yourself cluster ou à une solution entièrement gérée. Le contenu suivant présente certains des services de stockage fournis AWS pour une utilisation avec les instances Amazon EC2.

Table des matières

- [Utiliser Amazon S3 avec Amazon EC2](#)
- [Utiliser Amazon EFS avec des instances Linux](#)
- [Utiliser Amazon FSx avec Amazon EC2](#)
- [Utiliser Amazon File Cache avec Amazon EC2](#)

Utiliser Amazon S3 avec Amazon EC2

Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de pointe. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données pour différents cas d'utilisation, tels que les lacs de données, les sites Web, les sauvegardes et les analyses de mégadonnées, à partir d'une instance Amazon EC2 ou de n'importe où sur Internet. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon S3 ?](#)

Les objets sont les entités fondamentales stockées dans Amazon S3. Chaque objet stocké dans Amazon S3 se trouve dans un compartiment. Les compartiments organisent l'espace de noms Amazon S3 au plus haut niveau et identifient le compte qui assure ce stockage. Les compartiments Amazon S3 sont similaires aux noms de domaine Internet. Les objets stockés

dans les compartiments ont une valeur de clé unique et sont récupérés à l'aide d'une URL. Par exemple, si un objet avec la valeur de clé `/photos/mygarden.jpg` est stocké dans le compartiment `DOC-EXAMPLE-BUCKET1`, il est adressable à l'aide de l'URL `https://DOC-EXAMPLE-BUCKET1.s3.amazonaws.com/photos/mygarden.jpg`. Pour plus d'informations, consultez [Comment fonctionne Amazon S3](#).

Exemples d'utilisation :

Au vu des avantages qu'offre Amazon S3 pour le stockage, vous pouvez décider d'utiliser ce service pour stocker des fichiers et des ensembles de données à utiliser avec des instances EC2. Vous pouvez déplacer des données entre Amazon S3 et vos instances de différentes façons. En plus des exemples présentés ci-après, vous pouvez utiliser de nombreux outils conçus par des utilisateurs pour accéder à vos données dans Amazon S3 depuis votre ordinateur ou votre instance. Certains des plus courants sont présentés dans les forums AWS .

Si vous y êtes autorisé, vous pouvez copier un fichier vers ou depuis Amazon S3 et votre instance en utilisant l'une des méthodes suivantes.

GET or wget (Linux)

Note

Cette méthode ne fonctionne que pour les objets publics. Si l'objet n'est pas public, vous recevez un message `ERROR 403: Forbidden`. Si vous recevez cette erreur, vous devez utiliser la console Amazon S3 AWS CLI, AWS l'API, le AWS SDK ou AWS Tools for Windows PowerShell, et vous devez disposer des autorisations requises. Pour plus d'informations, consultez [Identity and Access Management dans Amazon S3](#) et [Téléchargement d'un objet](#) dans le Guide de l'utilisateur Amazon S3.

L'utilitaire `wget` est un client HTTP et FTP qui vous permet de télécharger des objets publics depuis Amazon S3. Il est installé par défaut dans Amazon Linux et la plupart des autres distributions, et est disponible en téléchargement sur Windows. Pour télécharger un objet Amazon S3, utilisez la commande suivante, en remplaçant l'URL par celle de l'objet à télécharger.

```
[ec2-user ~]$ wget https://my_bucket.s3.amazonaws.com/path-to-file
```

AWS Tools for Windows PowerShell (Windows)

Les instances Windows bénéficient d'un navigateur graphique que vous pouvez utiliser pour accéder directement à la console Amazon S3. Toutefois, dans le cadre du scripting, les utilisateurs Windows peuvent également utiliser [AWS Tools for Windows PowerShell](#) pour déplacer les objets depuis et vers Amazon S3.

Utilisez la commande suivante pour copier un objet Amazon S3 vers votre instance Windows.

```
PS C:\> Copy-S3Object -BucketName my_bucket -Key path-to-file -  
LocalFile my_copied_file.ext
```

AWS CLI (Linux and Windows)

Le AWS Command Line Interface (AWS CLI) est un outil unifié permettant de gérer vos AWS services. AWS CLI permet aux utilisateurs de s'authentifier et de télécharger des éléments restreints depuis Amazon S3, et également de charger des éléments. Pour plus d'informations notamment sur l'installation et la configuration des outils, consultez la [page détaillée sur l'AWS Command Line Interface](#).

La commande `aws s3 cp` est similaire à la commande Unix `cp`. Vous pouvez copier des fichiers depuis Amazon S3 vers votre instance, copier des fichiers depuis votre instance vers Amazon S3 et même copier des fichiers d'un emplacement Amazon S3 vers un autre.

Utilisez la commande suivante pour copier un objet depuis Amazon S3 vers votre instance.

```
aws s3 cp s3://my_bucket/my_folder/my_file.ext my_copied_file.ext
```

Utilisez la commande suivante pour copier un objet depuis votre instance vers Amazon S3.

```
aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

La commande `aws s3 sync` peut synchroniser un compartiment Amazon S3 entier vers un répertoire local. Cela peut être utile pour télécharger un ensemble de données et conserver la copie locale up-to-date avec la télécommande. Si vous disposez des autorisations adéquates sur le compartiment Amazon S3, vous pouvez renvoyer votre répertoire local sur le cloud lorsque vous avez terminé, en inversant les emplacements source et de destination dans la commande.

Utilisez la commande suivante pour télécharger un bucket Amazon S3 entier vers un répertoire local sur votre instance.

```
aws s3 sync s3://remote_S3_bucket local_directory
```

Amazon S3 API

Si vous êtes un développeur, vous pouvez utiliser une API pour accéder aux données dans Amazon S3. Vous pouvez utiliser cette API pour développer votre application et l'intégrer à d'autres API et SDK. Pour plus d'informations, consultez les [exemples de code pour Amazon S3 à l'aide de AWS kits SDK](#) dans le guide de l'utilisateur Amazon S3.

Utiliser Amazon EFS avec des instances Linux

Note

Amazon EFS n'est pas pris en charge par les instances Windows.

Amazon EFS offre un stockage de fichiers scalable, destiné à être utilisé avec Amazon EC2. Vous pouvez utiliser un système de fichiers EFS comme source de données commune aux charges de travail et applications exécutées sur plusieurs instances. Pour en savoir plus, consultez la [page produit d'Amazon Elastic File System](#).

Ce didacticiel explique comment créer et joindre un système de fichiers Amazon EFS à l'aide de l'assistant de création rapide Amazon EFS lors du lancement de l'instance. Pour un didacticiel sur la création d'un système de fichiers à l'aide de la console Amazon EFS, consultez [Mise en route avec Amazon Elastic File System](#) dans le guide de l'utilisateur Amazon Elastic File System.

Note

Lorsque vous créez un système de fichiers EFS à l'aide de la création rapide EFS, le système de fichiers est créé avec les paramètres recommandés par le service suivants :

- [Sauvegardes automatiques activées](#).
- [Montez les cibles dans chaque sous-réseau par défaut](#) du VPC sélectionné.
- [Mode de performance à usage général](#).
- [Mode haut débit](#).
- [Le chiffrement des données au repos est activé](#) à l'aide de votre clé par défaut pour Amazon EFS (aws/elasticfilesystem).

- La [gestion du cycle de vie Amazon EFS est activée](#) avec une politique de 30 jours.

Tâches

- [Créer un système de fichiers EFS à l'aide de la création rapide Amazon EFS](#)
- [Tester le système de fichiers EFS](#)
- [Supprimer le système de fichiers EFS](#)

Créer un système de fichiers EFS à l'aide de la création rapide Amazon EFS

Vous pouvez créer un système de fichiers EFS et le monter sur votre instance lorsque vous lancez votre instance à l'aide de la fonction de création rapide Amazon EFS de l'[assistant de lancement d'instance](#) Amazon EC2.

Pour créer un système de fichiers EFS à l'aide de la création rapide Amazon EFS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Sélectionnez Launch instance (Lancer une instance).
3. (Facultatif) Sous Name and tags (Noms et identifications), pour Name (Nom), saisissez un nom pour identifier votre instance.
4. Sous Application and OS Images (Amazon Machine Image) (Images d'application et de système d'exploitation), choisissez un système d'exploitation Linux, puis pour Amazon Machine Image (AMI), sélectionnez une AMI Linux.
5. Sous Instance type (Type d'instance), pour Instance type (Type d'instance), sélectionnez un type d'instance ou conservez la valeur par défaut.
6. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou créez-en une.
7. Sous Network settings (Paramètres réseau), choisissez Edit (Modifier) (à droite), puis pour Subnet (Sous-réseau), sélectionnez un sous-réseau.

Note

Vous devez sélectionner un sous-réseau avant de pouvoir ajouter un système de fichiers EFS.

8. Sous Configure storage (Configurer le stockage), choisissez Edit (Modifier) (en bas à droite), puis procédez comme suit :
 - a. Pour les systèmes de fichiers, assurez-vous que EFS est sélectionné, puis choisissez Créer un nouveau système de fichiers partagé.
 - b. Dans Nom du système de fichiers, entrez le nom du système de fichiers Amazon EFS, puis choisissez Create file system.
 - c. Pour Point de montage, spécifiez un point de montage personnalisé ou conservez le point de montage par défaut.
 - d. Pour permettre l'accès au système de fichiers, sélectionnez Automatically create and attach security groups (Créer et attacher automatiquement des groupes de sécurité). En cochant cette case, les groupes de sécurité suivants seront automatiquement créés et attachés à l'instance et aux cibles de montage du système de fichiers :
 - Groupe de sécurité d'instance : inclut une règle sortante qui autorise le trafic sur le port NFS 2049, mais aucune règle entrante.
 - Groupe de sécurité des cibles de montage du système de fichiers : comprend une règle entrante qui autorise le trafic sur le port NFS 2049 du groupe de sécurité de l'instance (décrit ci-dessus), et une règle sortante qui autorise le trafic sur le port NFS 2049.
 - e. Pour monter automatiquement le système de fichiers partagé lors du lancement de l'instance, sélectionnez Automatically mount shared file system by attaching required user data script (Monter automatiquement le système de fichiers partagé en attachant le script de données utilisateur requis). Pour afficher les données utilisateur générées automatiquement, développez Advanced details (Détails avancés), puis faites défiler vers le bas jusqu'à User data (Données utilisateur).

 Note

Vous pouvez également créer et associer manuellement les groupes de sécurité. Si vous voulez créer et attacher manuellement les groupes de sécurité, décochez la case Automatically create and attach the required security groups (Créer et attacher automatiquement les groupes de sécurité requis).

Note

Si vous avez ajouté des données utilisateur avant de cocher cette case, les données utilisateur d'origine sont remplacées par les données utilisateur générées automatiquement.

- Configurez les autres paramètres de configuration de l'instance si nécessaire.
- Dans le panneau Summary (Résumé), vérifiez la configuration de votre instance, puis choisissez Launch instance (Lancer l'instance). Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).

Tester le système de fichiers EFS

Vous pouvez vous connecter à votre instance et vérifier que le système de fichiers est bien monté dans le répertoire que vous avez indiqué (par exemple, /mnt/efs).

Pour vérifier que le système de fichiers est bien monté

- Connectez-vous à votre instance. Pour plus d'informations, consultez [Connectez-vous à votre instance Linux](#).
- Dans la fenêtre du terminal de l'instance, exécutez la commande `df -T` pour vérifier que le système de fichiers EFS est bien monté.

```
$ df -T
Filesystem      Type          1K-blocks    Used          Available Use% Mounted
on
/dev/xvda1      ext4          8123812 1949800          6073764 25% /
devtmpfs        devtmpfs      4078468     56          4078412  1% /dev
tmpfs           tmpfs         4089312     0           4089312  0% /dev/shm
efs-dns         nfs4          9007199254740992 0 9007199254740992 0% /mnt/efs
```

Notez que le nom du système de fichiers, qui s'affiche comme *efs-dns* dans l'exemple de résultat, est au format suivant.

```
file-system-id.efs.aws-region.amazonaws.com:/
```

- (Facultatif) Créez un fichier dans le système de fichiers à partir de l'instance, et vérifiez ensuite que vous pouvez consulter ce fichier à partir d'une autre instance.

- a. Depuis l'instance, exécutez la commande suivante pour créer le fichier.

```
$ sudo touch /mnt/efs/test-file.txt
```

- b. Depuis l'autre instance, exécutez la commande suivante pour afficher le fichier.

```
$ ls /mnt/efs  
test-file.txt
```

Supprimer le système de fichiers EFS

Si vous n'avez plus besoin de votre système de fichiers, vous pouvez le supprimer.

Pour supprimer le système de fichiers

1. Ouvrez la console Amazon Elastic File System à l'adresse <https://console.aws.amazon.com/efs/>.
2. Sélectionnez le système de fichiers à supprimer.
3. Choisissez Actions, Delete file system.
4. Lorsque vous êtes invité à confirmer, entrez l'ID du système de fichiers et choisissez Delete file system (Supprimer le système de fichiers).

Utiliser Amazon FSx avec Amazon EC2

La famille de services Amazon FSx facilite le lancement, l'exécution et la mise à l'échelle du stockage partagé alimenté par des systèmes de fichiers commerciaux et open source populaires. Vous pouvez utiliser l'assistant de lancement d'instance pour attacher automatiquement les types de systèmes de fichiers Amazon FSx suivants à vos instances Amazon EC2 au lancement :

- Amazon FSx for NetApp ONTAP fournit un stockage partagé entièrement géré dans le AWS cloud avec les fonctionnalités populaires d'accès aux données et de gestion d'ONTAP. NetApp
- Amazon FSx for OpenZFS fournit un stockage partagé économique entièrement géré, optimisé par le système de fichiers populaire OpenZFS.

Note

- Cette fonctionnalité est disponible uniquement dans l'assistant de lancement d'instance. Pour plus d'informations, consultez [Lancer une instance à l'aide du nouvel assistant de lancement d'instance](#).
- Les systèmes de fichiers Amazon FSx for Windows File Server et Amazon FSx pour Lustre ne peuvent pas être montés au lancement. Vous devez monter ces systèmes de fichiers manuellement après le lancement.

Vous pouvez choisir de monter un système de fichiers existant que vous avez créé précédemment, ou vous pouvez créer un nouveau système de fichiers à monter sur une instance au lancement.

Rubriques

- [Groupes de sécurité et script de données utilisateur](#)
- [Monter un système de fichiers Amazon FSx au lancement](#)

Groupes de sécurité et script de données utilisateur

Lorsque vous montez un système de fichiers Amazon FSx sur une instance à l'aide de l'assistant de lancement d'instance, vous pouvez choisir si les groupes de sécurité nécessaires à l'accès au système de fichiers sont créés et attachés automatiquement, et si les scripts de données utilisateur nécessaires au montage du système de fichiers sont automatiquement inclus et disponibles à l'utilisation.

Rubriques

- [Groupes de sécurité](#)
- [Script de données utilisateur](#)

Groupes de sécurité

Si vous choisissez de créer automatiquement les groupes de sécurité nécessaires pour activer l'accès au système de fichiers, l'assistant de lancement d'instance de lancement crée et attache deux groupes de sécurité : un groupe de sécurité est attaché à l'instance et l'autre est attaché au système de fichiers. Pour plus d'informations sur les exigences des groupes de sécurité, consultez [FSx for](#)

[ONTAP file system access control with Amazon VPC](#) et [FSx for OpenZFS file system access control with Amazon VPC](#).

Nous ajoutons la balise `Name=instance-sg-1` au groupe de sécurité créé et attaché à l'instance. La valeur de la balise est automatiquement incrémentée chaque fois que l'assistant de lancement d'instance crée un groupe de sécurité pour les systèmes de fichiers Amazon FSx.

Le groupe de sécurité comprend les règles de sortie suivantes, mais aucune règle d'entrée.

Règles sortantes

Type de protocole	Numéro de port	Destination
UDP	111	<i>groupe de sécurité du système de fichiers</i>
UDP	2001 - 2003	<i>groupe de sécurité du système de fichiers</i>
UDP	4049	<i>groupe de sécurité du système de fichiers</i>
UDP	2049	<i>groupe de sécurité du système de fichiers</i>
UDP	635	<i>groupe de sécurité du système de fichiers</i>
UDP	4045 - 4046	<i>groupe de sécurité du système de fichiers</i>
TCP	4049	<i>groupe de sécurité du système de fichiers</i>
TCP	635	<i>groupe de sécurité du système de fichiers</i>
TCP	2049	<i>groupe de sécurité du système de fichiers</i>

Type de protocole	Numéro de port	Destination
TCP	111	<i>groupe de sécurité du système de fichiers</i>
TCP	4045 - 4046	<i>groupe de sécurité du système de fichiers</i>
TCP	2001 - 2003	<i>groupe de sécurité du système de fichiers</i>
Tous	Tous	<i>groupe de sécurité du système de fichiers</i>

Le groupe de sécurité créé et attaché au système de fichiers est balisé avec Name=fsx-sg-**1**. La valeur de la balise est automatiquement incrémentée chaque fois que l'assistant de lancement d'instance crée un groupe de sécurité pour les systèmes de fichiers Amazon FSx.

Le groupe de sécurité comprend les règles suivantes.

Règles entrantes

Type de protocole	Numéro de port	Source
UDP	2049	<i>groupe_sécurité_instances</i>
UDP	2001 - 2003	<i>groupe_sécurité_instances</i>
UDP	4049	<i>groupe_sécurité_instances</i>
UDP	111	<i>groupe_sécurité_instances</i>
UDP	635	<i>groupe_sécurité_instances</i>
UDP	4045 - 4046	<i>groupe_sécurité_instances</i>
TCP	4045 - 4046	<i>groupe_sécurité_instances</i>
TCP	635	<i>groupe_sécurité_instances</i>

Type de protocole	Numéro de port	Source
TCP	2049	<i>groupe_sécurité_instances</i>
TCP	4049	<i>groupe_sécurité_instances</i>
TCP	2001 - 2003	<i>groupe_sécurité_instances</i>
TCP	111	<i>groupe_sécurité_instances</i>

Règles sortantes

Type de protocole	Numéro de port	Destination
Tous	Tous	0.0.0.0/0

Script de données utilisateur

Si vous choisissez d'attacher automatiquement des scripts de données utilisateur, l'assistant de lancement d'instance ajoute les données utilisateur suivantes à l'instance. Ce script installe les packages nécessaires, monte le système de fichiers et met à jour les paramètres de votre instance afin que le système de fichiers soit automatiquement remonté chaque fois que l'instance redémarre.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "${svm_id_1}" ]; then printf "\n${file_system_id_1}.fsx.eu-north-1.amazonaws.com/${vol_path_1} ${fsx_mount_point_1} nfs4
nfsvers=4.1,rsz=1048576,wsz=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-north-1.amazonaws.com/${vol_path_1} ${fsx_mount_point_1} nfs4
```

```
nfsvers=4.1,rsize=1048576,wsiz=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
[ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Monter un système de fichiers Amazon FSx au lancement

Pour monter un système de fichiers Amazon FSx nouveau ou existant au lancement

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances, Launch instance (Lancer l'instance) pour ouvrir l'assistant de lancement d'instance.
3. Dans la section Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez l'AMI à utiliser.
4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance.
5. Pour la section Key pair (Paire de clés), sélectionnez une paire de clés existante ou créez-en une nouvelle.
6. Dans la section Network settings (Paramètres réseau), procédez comme suit :
 - a. Choisissez Modifier.
 - b. Si vous souhaitez monter un système de fichiers existant, pour Subnet (Sous-réseau), choisissez le sous-réseau préféré du système de fichiers. Nous vous recommandons de lancer l'instance dans la même zone de disponibilité que le sous-réseau préféré du système de fichiers afin d'optimiser les performances.

Si vous souhaitez créer un nouveau système de fichiers à monter sur une instance, pour Subnet (Sous-réseau), choisissez le sous-réseau dans lequel lancer l'instance.

Important

Vous devez sélectionner un sous-réseau pour activer la fonctionnalité Amazon FSx dans l'assistant de nouvelle instance de lancement. Si vous ne sélectionnez pas de sous-réseau, vous ne pourrez pas monter un système de fichiers existant ou en créer un nouveau.

7. Dans la section Storage (Stockage), procédez comme suit :

- a. Configurez les volumes au besoin.
- b. Développez la section File systems (Systèmes de fichiers) et sélectionnez FSx.
- c. Choisissez Add shared file system (Ajouter un système de fichiers partagé).
- d. Pour File system (Système de fichiers), sélectionnez le système de fichiers à monter.

 Note

La liste affiche tous les systèmes de fichiers Amazon FSx pour NetApp ONTAP et Amazon FSx pour OpenZFS de votre compte dans la région sélectionnée.

- e. Pour créer et attacher automatiquement les groupes de sécurité nécessaires à l'accès au système de fichiers, sélectionnez Automatically create and attach security groups (Créer et attacher automatiquement des groupes de sécurité). Si vous préférez créer manuellement les groupes de sécurité, décochez la case. Pour plus d'informations, consultez [Groupes de sécurité](#).
 - f. Pour attacher automatiquement les scripts de données utilisateur nécessaires au montage du système de fichiers, sélectionnez Automatically mount shared file system by attaching required user data script (Monter automatiquement le système de fichiers partagé en attachant le script de données utilisateur requis). Si vous préférez fournir manuellement les scripts de données utilisateur, décochez la case. Pour plus d'informations, consultez [Script de données utilisateur](#).
8. Dans Advanced (Avancé), configurez les paramètres d'instance supplémentaires au besoin.
 9. Choisissez Lancer.

Utiliser Amazon File Cache avec Amazon EC2

Amazon File Cache est un cache haut débit entièrement géré AWS qui est utilisé pour traiter les données des fichiers, quel que soit leur emplacement de stockage. Amazon File Cache sert d'emplacement de stockage temporaire à hautes performances pour les données stockées dans des systèmes de fichiers locaux, des systèmes de fichiers AWS et des compartiments Amazon Simple Storage Service (Amazon S3). Vous pouvez utiliser cette fonctionnalité pour mettre des ensembles de données dispersés à la disposition des applications basées sur des fichiers AWS avec une vue unifiée et à des vitesses élevées (latences inférieures à la milliseconde et débit élevé). Pour plus d'informations, consultez [Qu'est-ce qu'Amazon File Cache ?](#).

Vous pouvez accéder à votre cache depuis vos instances Amazon EC2 à l'aide du client Lustre open source. Les instances Amazon EC2 peuvent accéder à votre cache depuis d'autres zones de disponibilité au sein du même Amazon Virtual Private Cloud (Amazon VPC), à condition que votre réseau autorise l'accès via les sous-réseaux du VPC. Une fois votre cache monté, vous pouvez travailler avec ses fichiers et ses répertoires comme vous le feriez avec un système de fichiers local.

Pour commencer, consultez [Getting started with Amazon File Cache](#).

Limites de volume d'instance

Le nombre maximal de volumes Amazon EBS que vous pouvez associer à une instance dépend du type et de la taille de l'instance. Lorsque vous réfléchissez au nombre de volumes à attacher à votre instance, vous devriez déterminer si vous avez besoin d'une plus grande bande passante E/S ou d'une plus grande capacité de stockage.

Bande passante et capacité

Pour des cas d'utilisation de bande passante cohérents et prévisibles, utilisez des instances optimisées pour Amazon EBS avec des volumes SSD à usage général ou des volumes SSD IOPS provisionnés. Pour des performances maximales, associez les E/S par seconde que vous avez provisionnées pour vos volumes et la bande passante disponible pour votre type d'instance.

Pour les configurations RAID, vous constaterez que des grappes de plus de huit volumes diminuent les retours de performances en raison d'une plus grande surcharge E/S. Testez la performance de votre application individuelle et ajustez-la si nécessaire.

Rubriques

- [Limites de volume pour les instances créées sur le système Nitro](#)
- [Limites de volume pour les instances basées sur Xen](#)

Limites de volume pour les instances créées sur le système Nitro

Rubriques

- [Limite de volume Amazon EBS dédiée](#)
- [Limite de volume Amazon EBS partagée](#)

Limite de volume Amazon EBS dédiée

Les types d'instances Nitro suivants ont une limite de volume Amazon EBS dédiée qui varie en fonction de la taille de l'instance. La limite n'est pas partagée avec les autres pièces jointes du périphérique. En d'autres termes, vous pouvez attacher n'importe quel nombre de volumes Amazon EBS jusqu'à la limite de pièces jointes, quel que soit le nombre de périphériques connectés, tels que les volumes de stockage d'instance NVMe et les interfaces réseau.

- Usage général : M7a, M7i, M7i-Flex
- Optimisée pour le calcul : C7a, C7i
- Optimisées pour la mémoire : R7a, R7i, R7iz

Pour les types d'instances qui prennent en charge les limites de volume dédiées, les limites de volume dépendent de la taille de l'instance. Le tableau suivant indique la limite de chaque taille d'instance.

Taille d'instance	Limite de volume
medium large xlarge 2xlarge 4xlarge 8xlarge 12xlarge	32
16xlarge	48
24xlarge	64
32xlarge	88
48xlarge	128
metal-16x1 metal-24x 1	39
metal-32x1 metal-48x 1	79

Limite de volume Amazon EBS partagée

Tous les autres types d'instances Nitro (non répertoriés dans [Limite de volume Amazon EBS dédiée](#)) ont une limite d'attachement de volume partagée entre les volumes Amazon EBS, les interfaces réseau et les volumes de stockage d'instances NVMe. Vous pouvez attacher n'importe quel nombre de volumes Amazon EBS jusqu'à cette limite, moins le nombre d'interfaces réseau et de volumes de stockage d'instance NVMe attachés. N'oubliez pas que chaque instance doit disposer d'au moins une interface réseau et que les volumes de stockage d'instance NVMe sont automatiquement attachés au lancement.

La plupart de ces instances prennent en charge un maximum de 28 attachements. Si, par exemple, vous ne possédez pas d'interfaces réseau supplémentaires attachées sur une instance `m5.xlarge`, vous pouvez attacher jusqu'à 27 volumes EBS (limite de 28 volumes - 1 interface réseau). Si vous disposez de deux interfaces réseau supplémentaires sur une instance `m5.xlarge`, vous pouvez attacher jusqu'à 25 volumes EBS (limite de 28 volumes - 3 interfaces réseau). De même, si vous disposez de deux interfaces réseau supplémentaires sur une instance `m5d.xlarge`, qui possède 1 volume de stockage d'instance NVMe, vous pouvez attacher jusqu'à 24 volumes EBS (limite de 28 volumes - 3 interfaces réseau - 1 volume de stockage d'instance NVMe).

Les exceptions suivantes concernent les types d'instances dont les limites de volume sont partagées :

- Les instances `DL2q` prennent en charge jusqu'à 19 volumes EBS.
- La plupart des instances matériel nu prennent en charge un maximum de 31 volumes EBS.
- Les instances virtualisées à mémoire élevée prennent en charge un maximum de 27 volumes EBS.
- Les instances nues à mémoire élevée prennent en charge un maximum de 19 volumes EBS.
- Les instances `inf1.xlarge` et `inf1.2xlarge`, prennent en charge jusqu'à 26 volumes EBS.
- `inf1.6xlarge` Les instances prennent en charge jusqu'à 23 volumes EBS.
- `mac1.metal` Les instances prennent en charge jusqu'à 16 volumes EBS.
- `mac2.metal`, `mac2-m2.metal`, et les `mac2-m2pro.metal` instances prennent en charge un maximum de 10 volumes EBS.
- `inf1.24xlarge` Les instances prennent en charge 11 volumes EBS maximum.
- `g5.48xlarge` Les instances prennent en charge jusqu'à 9 volumes EBS.
- Les instances `d3.8xlarge` et `d3en.12xlarge` prennent en charge jusqu'à 3 volumes EBS.
- Pour les instances de calcul accéléré, les accélérateurs attachés sont pris en compte dans le calcul de la limite de volume partagé. Par exemple, pour les instances `p4d.24xlarge`, qui ont une

limite de volume partagé de 28, 8 GPU et 8 volumes de stockage d'instance NVMe, vous pouvez attacher jusqu'à 11 volumes Amazon EBS (limite de 28 volumes - 1 interface réseau - 8 GPU - 8 volumes de stockage d'instance NVMe).

Limites de volume pour les instances basées sur Xen

Instances Linux

L'attachement de plus de 40 volumes à une instance Linux basée sur Xen peut provoquer des échecs de démarrage. Ce nombre inclut le volume racine, ainsi que tous les volumes de stockage d'instance et les volumes Amazon EBS attachés.

Si vous rencontrez des problèmes de démarrage sur une instance avec un grand nombre de volumes, arrêtez l'instance, détachez tous les volumes qui ne sont pas essentiels au processus de démarrage, démarrez l'instance, puis rattachés les volumes une fois que l'instance est en cours d'exécution.

Important

Attacher plus de 40 volumes sur une instance Linux basée sur Xen est pris en charge autant que possible et ce, sans garantie.

instances Windows

Le tableau ci-après affiche les limites de volumes pour les instances Windows basées sur Xen en fonction du pilote utilisé. Veuillez noter que ces nombres incluent le volume racine, ainsi que tous les volumes de stockage d'instance et les volumes Amazon EBS attachés.

Important

Attacher plus que le nombre de volumes suivant sur une instance Windows basée sur Xen est pris en charge autant que possible et ce, sans garantie.

Pilote	Limite de volume
AWS PV	26

Pilote	Limite de volume
Virtualisation paravirtuelle Citrix	26
Virtualisation paravirtuelle Red Hat	17

Nous vous recommandons de ne pas associer plus de 26 volumes à une instance Windows basée sur XEN avec des pilotes AWS PV ou Citrix PV, car cela pourrait entraîner des problèmes de performances. Pour déterminer quels pilotes de virtualisation paravirtuelle sont utilisés par votre instance, ou pour passer votre instance Windows de pilotes de virtualisation paravirtuelle Red Hat à des pilotes Citrix, veuillez consulter la rubrique [the section called “Mettre à niveau les pilotes PV”](#).

Pour plus d'informations sur la façon dont les noms de périphériques sont liés aux volumes, veuillez consulter la rubrique [Mapper des disques sur des volumes sur votre instance Windows](#).

Volume racine de l'instance Amazon EC2

Lorsque vous lancez une instance, nous créons un volume racine pour l'instance. Le volume racine contient l'image utilisée pour démarrer l'instance. Chaque instance possède un volume racine unique. Vous pouvez ajouter des volumes de stockage à vos instances pendant ou après le lancement.

Nous réservons des noms de périphérique spécifiques aux volumes racines. Pour plus d'informations, consultez [Noms des appareils sur les instances Amazon EC2](#).

Table des matières

- [Type de volume racine](#)
- [Choisissez une AMI Linux par type de volume racine](#)
- [Déterminez le type de périphérique racine de votre instance Linux](#)
- [Modifier le volume racine pour qu'il persiste](#)
- [Modifier la taille initiale du volume racine](#)
- [Remplacer un volume racine d'instance EC2](#)

Type de volume racine

L'AMI que vous utilisez pour lancer une instance détermine le type de volume racine. Vous pouvez lancer une instance à partir d'une AMI basée sur Amazon EBS (instances Linux et Windows) ou

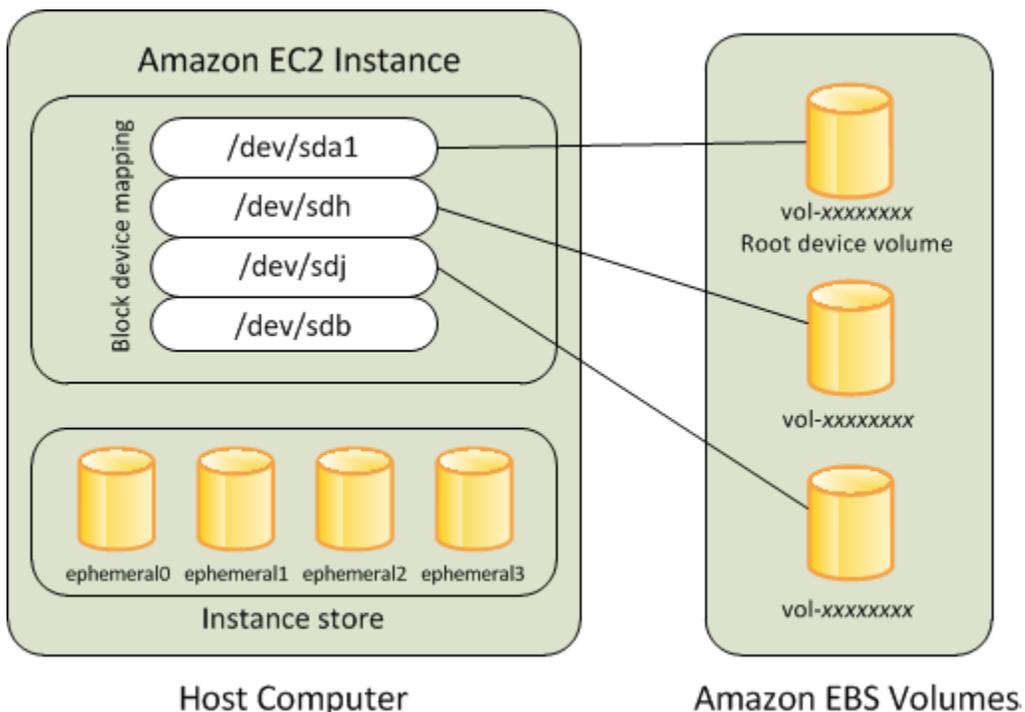
d'une AMI basée sur un stockage d'instance (instances Linux uniquement). Il existe des différences importantes entre ce que vous pouvez faire avec chaque type d'AMI. Pour plus d'informations sur ces différences, consultez [Stockage pour le périphérique racine](#).

Il est recommandé d'utiliser les AMI basées sur les volumes Amazon EBS, car ces instances se lancent plus rapidement et utilisent le stockage permanent.

instances basées sur les volumes Amazon EBS

Les instances qui ont recours à Amazon EBS pour le volume racine sont automatiquement associées à un volume Amazon EBS. Lorsque vous lancez une instance basée sur les volumes Amazon EBS, nous créons un volume Amazon EBS pour chaque instantané Amazon EBS référencé par l'AMI que vous utilisez. Vous pouvez aussi utiliser d'autres volumes Amazon EBS ou des volumes de stockage d'instance, suivant le type d'instance.

Une instance basée sur Amazon EBS peut être arrêtée et redémarrée ultérieurement sans affecter les données stockées dans les volumes attachés. Il existe diverses tâches liées aux instances et aux volumes que vous pouvez effectuer quand une instance basée sur Amazon EBS est dans un état arrêté. Par exemple, vous pouvez modifier les propriétés de l'instance, changer sa taille ou mettre à jour le noyau qu'elle utilise, ou vous pouvez aussi attacher votre volume racine à une autre instance en cours d'exécution à des fins de débogage ou autre. Pour plus d'informations, consultez la section [Amazon EBS volumes](#).



Limitation

Vous ne pouvez pas utiliser de volumes EBS st1 ou sc1 en tant que volumes racines.

Défaillance de l'instance

Si une instance basée sur Amazon EBS échoue, vous pouvez restaurer votre session en suivant l'une de ces méthodes :

- Arrêtez l'instance et redémarrez-la (essayez cette méthode en premier).
- Prenez automatiquement un instantané de tous les volumes appropriés et créez un nouvel AMI. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).
- Attachez le volume à la nouvelle instance à l'aide des étapes suivantes :
 1. Créez un instantané du volume racine.
 2. Inscrivez un nouvel AMI à l'aide de l'instantané.
 3. Lancez une nouvelle instance à partir du nouvel AMI.
 4. Détachez les volumes Amazon EBS restants de l'ancienne instance.
 5. Rattachez les volumes Amazon EBS à la nouvelle instance.

Instances basées sur le stockage d'instances (instances Linux uniquement)

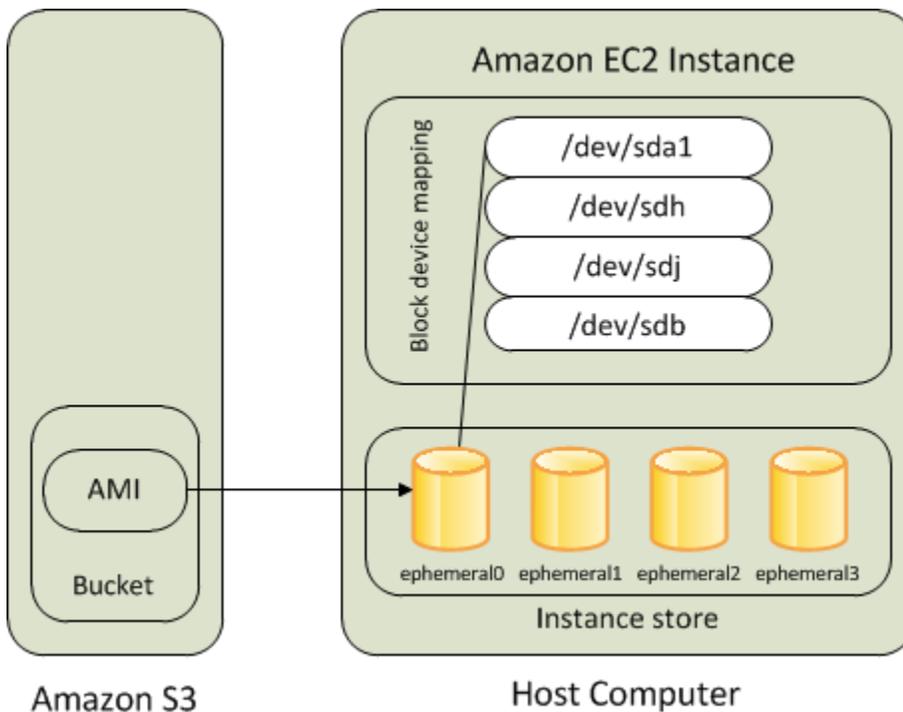
Note

Les instances Windows ne prennent pas en charge les volumes racine sauvegardés par le stockage d'instances.

Les instances qui utilisent les stockages d'instance pour le volume racine ont automatiquement un ou plusieurs volumes de stockage d'instance disponibles, l'un faisant office de volume racine. Quand une instance est lancée, l'image utilisée pour démarrer l'instance est copiée sur le volume racine. Notez que vous pouvez utiliser le cas échéant des volumes de stockage d'instance supplémentaires, suivant le type d'instance.

Les données présentes sur les volumes de stockage d'instance demeurent aussi longtemps que l'instance s'exécute, mais ces données sont supprimées quand il est procédé à la terminaison de l'instance (les instances basées sur le stockage d'instance ne prennent pas en charge l'action

Stop) ou en cas de défaillance de l'instance (problèmes rencontrés par un lecteur sous-jacent, par exemple). Pour plus d'informations, consultez [Stockage d'instances Amazon EC2](#).



Exigence

Seuls les types d'instance suivants prennent en charge un volume de stockage d'instance en tant que volume racine : C3, D2, I2, M3 et R3.

Défaillance de l'instance

Après qu'une instance basée sur le stockage d'instances a échoué ou s'est terminée, elle ne peut pas être restaurée. Si vous prévoyez d'utiliser les instances basées sur le stockage d'instance Amazon EC2, il est vivement recommandé de répartir les données de vos stockages d'instance entre plusieurs zones de disponibilité. Vous devez aussi sauvegarder régulièrement les données critiques de vos volumes de stockage d'instance sur un stockage permanent.

Choisissez une AMI Linux par type de volume racine

Note

Toutes les AMI Windows sont basées sur EBS.

L'AMI que vous spécifiez au lancement de votre instance détermine le type de volume du périphérique racine de votre instance. Vous pouvez afficher les AMI par type de périphérique racine à l'aide de l'une des méthodes suivantes.

Console

Pour choisir une AMI basée sur des volumes Amazon EBS avec la console

1. Ouvrez la console Amazon EC2.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Dans les listes de filtres, sélectionnez le type d'image (par exemple, Public images). Dans la barre de recherche, choisissez Platform pour sélectionner le système d'exploitation (tel qu'Amazon Linux) et Root devicetype pour sélectionner le type de volume racine (ebs ou instance-store).
4. (Facultatif) Pour obtenir des informations supplémentaires afin de vous aider à choisir, choisissez l'icône Préférences, activez les colonnes à afficher et choisissez Confirmer.
5. Choisissez une AMI et notez l'ID d'AMI.

AWS CLI

Pour vérifier le volume du périphérique racine d'une AMI à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur ces interfaces ligne de commande, consultez [Accès à Amazon EC2](#).

- [describe-images](#) (AWS CLI)
- [Get-EC2Image](#) (AWS Tools for Windows PowerShell)

Déterminez le type de périphérique racine de votre instance Linux

Note

Toutes les instances Windows sont basées sur EBS.

Vous pouvez afficher le type de périphérique racine de votre instance Linux à l'aide de l'une des méthodes suivantes.

Console

Pour déterminer le type de périphérique racine d'une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances, puis choisissez l'instance.
3. Sous l'onglet Stockage, sous Détails de l'appareil racine, vérifiez la valeur de Type d'appareil racine comme suit :
 - Si la valeur est EBS, il s'agit d'une instance basée sur Amazon EBS.
 - Si la valeur est INSTANCE-STORE, il s'agit d'une instance basée sur le stockage d'instance.

AWS CLI

Pour déterminer le type de périphérique racine d'une instance à l'aide de la ligne de commande

Vous pouvez utiliser l'une des commandes suivantes. Pour obtenir plus d'informations sur les CLI (interface ligne de commande), consultez le didacticiel [Accès à Amazon EC2](#).

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (AWS Tools for Windows PowerShell)

Modifier le volume racine pour qu'il persiste

Par défaut, le volume racine d'une AMI basée sur Amazon EBS est supprimé quand l'instance se termine. Vous pouvez modifier le comportement par défaut pour vous assurer que le volume persiste après la fin de l'instance. Pour modifier le comportement par défaut, définissez l'attribut `DeleteOnTermination` avec la valeur `false` à l'aide d'un mappage de périphérique de stockage en mode bloc.

Tâches

- [Configurer le volume racine pour qu'il persiste pendant le lancement de l'instance](#)
- [Configurer le volume racine pour qu'il persiste pour une instance existante](#)
- [Confirmer qu'un volume racine est configuré pour persister](#)

Configurer le volume racine pour qu'il persiste pendant le lancement de l'instance

Vous pouvez configurer le volume racine pour qu'il persiste lorsque vous lancez une instance à l'aide de la console Amazon EC2 ou des outils de ligne de commande.

Console

Configurer le volume racine pour qu'il persiste lorsque vous lancez une instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances, puis Lancer une instance.
3. Choisissez une Amazon Machine Image (AMI), choisissez un type d'instance, choisissez une paire de clés et configurez vos paramètres réseau.
4. Pour Configurer le stockage, choisissez Avancé.
5. Développez le volume racine.
6. Pour Supprimer à la résiliation, choisissez Non.
7. Une fois la configuration de votre instance terminée, choisissez Lancer l'instance.

AWS CLI

Pour configurer le volume racine de manière à ce qu'il persiste lorsque vous lancez une instance à l'aide du AWS CLI

Utilisez la commande [run-instances](#) et incluez un mappage de périphérique en mode bloc qui définit l'attribut `DeleteOnTermination` avec la valeur `false`.

```
aws ec2 run-instances --block-device-mappings file://mapping.json ...other
parameters...
```

Spécifiez les éléments suivants dans `mapping.json`.

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

```
]
```

Tools for Windows PowerShell

Pour configurer le volume racine de manière à ce qu'il persiste lorsque vous lancez une instance à l'aide des Outils pour Windows PowerShell

Utilisez la [New-EC2Instance](#) commande et incluez un mappage de périphériques en mode bloc qui définit l'attribut `DeleteOnTermination` sur `false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
C:\> $bdm.DeviceName = "dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> New-EC2Instance -ImageId ami-0abcdef1234567890 -BlockDeviceMapping
$bdm ...other parameters...
```

Configurer le volume racine pour qu'il persiste pour une instance existante

Vous pouvez configurer le volume racine pour qu'il persiste pour une instance en cours d'exécution à l'aide des outils de ligne de commande uniquement.

AWS CLI

Pour configurer le volume racine de manière à ce qu'il soit conservé pour une instance existante à l'aide du AWS CLI

Utilisez la commande [modify-instance-attribute](#) et incluez un mappage de périphérique en mode bloc qui définit l'attribut `DeleteOnTermination` sur `false`.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-
mappings file://mapping.json
```

Spécifiez les éléments suivants dans `mapping.json`.

```
[
  {
    "DeviceName": "/dev/xvda",
    "Ebs": {
```

```
        "DeleteOnTermination": false
      }
    }
  ]
}
```

Tools for Windows PowerShell

Configurer le volume racine pour qu'il persiste pour une instance existante à l'aide de AWS Tools for Windows PowerShell

Utilisez la [Edit-EC2InstanceAttribute](#) commande avec un mappage de périphériques en mode bloc qui définit l'`DeleteOnTermination` attribut sur `false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
C:\> $bdm.DeviceName = "/dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -BlockDeviceMapping
    $bdm
```

Confirmer qu'un volume racine est configuré pour persister

Vous pouvez confirmer qu'un volume racine est configuré pour persister à l'aide de la console Amazon EC2 ou des outils de ligne de commande.

Console

Confirmer qu'un volume racine est configuré pour persister à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances, puis sélectionnez l'instance.
3. Dans l'onglet Stockage, sous Bloquer les appareil, recherchez l'entrée du volume racine. Si la valeur Supprimer lors de la résiliation est définie avec la valeur No, le volume est configuré pour persister.

AWS CLI

Pour confirmer qu'un volume racine est configuré pour persister à l'aide du AWS CLI

Utilisez la commande [describe-instances](#) et vérifiez que l'attribut `DeleteOnTermination` de l'élément de réponse `BlockDeviceMappings` est défini avec la valeur `false`.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

```
...
  "BlockDeviceMappings": [
    {
      "DeviceName": "/dev/sda1",
      "Ebs": {
        "Status": "attached",
        "DeleteOnTermination": false,
        "VolumeId": "vol-1234567890abcdef0",
        "AttachTime": "2013-07-19T02:42:39.000Z"
      }
    }
  ]
...

```

Tools for Windows PowerShell

Pour confirmer qu'un volume racine est configuré pour persister à l'aide du AWS Tools for Windows PowerShell

Utilisez le [Get-EC2Instance](#) et vérifiez que l'attribut `DeleteOnTermination` de l'élément de réponse `BlockDeviceMappings` est défini sur `false`.

```
C:\> (Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Modifier la taille initiale du volume racine

Par défaut, la taille du volume racine est déterminée par la taille de l'instantané. Vous pouvez augmenter la taille initiale du volume racine en utilisant le mappage de périphérique de stockage en mode bloc de l'instance comme suit.

1. Déterminez le nom du périphérique du volume racine spécifié dans l'AMI, comme décrit dans [Afficher les volumes EBS dans un mappage de périphérique de stockage en mode bloc d'une AMI](#).
2. Vérifiez la taille de l'instantané spécifiée dans le mappage des périphériques par blocs AMI.

3. Remplacez la taille du volume racine à l'aide du mappage de périphérique de stockage en mode bloc d'instance, comme décrit dans [Mettre à jour le mappage de périphérique de stockage en mode bloc lors du lancement d'une instance](#), en spécifiant une taille de volume supérieure à la taille de l'instantané.

Par exemple, l'entrée suivante pour le mappage de périphérique de stockage en mode bloc d'instance augmente la taille du volume racine, /dev/xvda, à 100 Gio. Vous pouvez omettre l'ID d'instantané dans le mappage de périphérique de stockage en mode bloc d'instance car l'ID d'instantané est déjà spécifié dans le mappage de périphérique de stockage en mode bloc d'AMI.

```
{
  "DeviceName": "/dev/xvda",
  "Ebs": {
    "VolumeSize": 100
  }
}
```

Pour plus d'informations, consultez [Mappages de périphériques de stockage en mode bloc](#).

Remplacer un volume racine d'instance EC2

Amazon EC2 vous permet de remplacer le volume EBS racine d'une instance en cours d'exécution tout en conservant les éléments suivants :

- Données stockées sur les volumes de stockage d'instance — Les volumes de stockage d'instances restent attachés à l'instance après la restauration du volume racine.
- Données stockées sur les volumes de données (non racine) d'Amazon EBS — Les volumes Amazon EBS non racine restent attachés à l'instance après la restauration du volume racine.
- Configuration réseau — Toutes les interfaces réseau restent attachées à l'instance et conservent leur adresses IP, leurs identifiants et leurs ID d'attachement. Lorsque l'instance devient disponible, tout le trafic réseau en attente est purgé. En outre, l'instance reste sur le même hôte physique, ce qui lui permet de conserver ses adresses IP publiques et privées ainsi que son nom DNS.
- Stratégies IAM — Les profils et politiques IAM (tels que les politiques basées sur des balises) associés à l'instance sont conservés et appliqués.

Rubriques

- [Fonctionnement](#)

- [Remplacer un volume racine](#)
- [Afficher les tâches de remplacement du volume racine](#)

Fonctionnement

Lorsque vous remplacez le volume racine d'une instance, un nouveau volume racine (de remplacement) est restauré de l'une des manières suivantes :

- À l'état de lancement initial : le volume est restauré à son état initial lors du lancement de l'instance. Pour plus d'informations, consultez [Restauration d'un volume racine à son état de lancement](#).
- À partir d'un instantané de la même lignée que le volume racine actuel : cela vous permet de résoudre les problèmes, tels que la corruption du volume racine ou les erreurs de configuration réseau du système d'exploitation invité. Pour plus d'informations, consultez [Remplacement d'un volume racine à l'aide d'un instantané](#).
- À partir d'une AMI qui possède les mêmes attributs clés que l'instance : cela vous permet d'appliquer des correctifs ou d'effectuer des mises à niveau du système d'exploitation et des applications. Pour plus d'informations, consultez [Remplacement d'un volume racine à l'aide d'une AMI](#).

Le volume racine d'origine est détaché de l'instance et le nouveau volume racine est attaché à l'instance à sa place. Le mappage de périphérique de stockage en mode bloc de l'instance est mis à jour pour refléter l'ID du volume racine de remplacement. Vous pouvez choisir de conserver ou non le volume racine d'origine une fois le processus de remplacement de celui-ci terminé. Si vous choisissez de supprimer le volume racine d'origine une fois le processus de remplacement terminé, le volume racine d'origine est automatiquement supprimé et devient irrécupérable. Si vous choisissez de conserver le volume racine d'origine une fois le processus terminé, le volume reste provisionné dans votre compte ; vous devez le supprimer manuellement lorsque vous n'en avez plus besoin.

Si la tâche de remplacement du volume racine échoue, l'instance est redémarrée et le volume racine d'origine reste attaché à l'instance.

Considérations relatives au remplacement du volume racine

- L'instance doit être dans l'état `running`.
- L'instance est automatiquement redémarrée pendant le processus. Le contenu de la mémoire (RAM) est effacé lors du redémarrage. Aucun redémarrage manuel n'est nécessaire.

- Vous ne pouvez pas remplacer le volume racine s'il s'agit d'un volume de stockage d'instances. Seules les instances avec des volumes racines Amazon EBS sont prises en charge.
- Vous pouvez remplacer le volume racine pour tous les types d'instances virtualisées et les instances matériel nu EC2 Mac. Tous les autres types d'instances matériel nu ne sont pas pris en charge.
- Vous pouvez utiliser n'importe quel instantané qui appartient à la même lignée que l'un des volumes racine précédents de l'instance.
- Si votre compte est activé pour le Chiffrement Amazon EBS par défaut dans la région actuelle, le volume racine de remplacement créé par la tâche de remplacement du volume racine est toujours chiffré, quel que soit l'état de chiffrement de l'instantané spécifié ou du volume racine de l'AMI spécifiée.
- Le tableau suivant récapitule les résultats de chiffrement possibles.

	Volume racine d'origine	Instantané ou AMI spécifié	Chiffrement par défaut	Remplacement du volume racine	Clé de chiffrement utilisée pour le volume racine de remplacement
Restaurer le volume racine de remplacement à l'état de lancement initial	Chiffré	Ne s'applique pas	Non pris en compte	Chiffré	Même clé KMS que le volume racine d'origine
	Non chiffré	Ne s'applique pas	Désactivées	Non chiffré	Ne s'applique pas
	Non chiffré	Ne s'applique pas	Activées	Chiffré	Clé KMS par défaut du compte pour le chiffrement Amazon EBS

	Volume racine d'origine	Instantané ou AMI spécifié	Chiffrement par défaut	Remplacement du volume racine	Clé de chiffrement utilisée pour le volume racine de remplacement
Restauration du volume racine de remplacement à partir d'un instantané ou d'une AMI	Chiffré	Non chiffré	Non pris en compte	Chiffré	Même clé KMS que le volume racine d'origine
	Chiffré	Chiffré	Non pris en compte	Chiffré	Même clé KMS que le volume racine d'origine
	Non chiffré	Non chiffré	Désactivées	Non chiffré	Ne s'applique pas
	Non chiffré	Non chiffré	Activées	Chiffré	Clé KMS par défaut du compte pour le chiffrement Amazon EBS

	Volume racine d'origine	Instantané ou AMI spécifié	Chiffrement par défaut	Remplacement du volume racine	Clé de chiffrement utilisée pour le volume racine de remplacement
	Non chiffré	Chiffré	Non pris en compte	Chiffré	Si l'AMI ou l'instantané appartient au compte, le volume de remplacement est chiffré à l'aide de la clé KMS de l'AMI ou de l'instantané. Si une AMI ou un instantané est partagé avec le compte, le volume de remplacement est chiffré avec la clé KMS par défaut pour le chiffrement Amazon EBS du compte.

Rubriques

- [Restauration d'un volume racine à son état de lancement](#)
- [Remplacement d'un volume racine à l'aide d'un instantané](#)
- [Remplacement d'un volume racine à l'aide d'une AMI](#)

Restauration d'un volume racine à son état de lancement

Vous pouvez procéder à un remplacement de volume racine qui consiste à remplacer le volume racine d'une instance par un volume racine de remplacement qui est restauré à l'état de lancement du volume racine d'origine. Le volume de remplacement est automatiquement restauré à partir de l'instantané utilisé pour créer le volume d'origine lors du lancement de l'instance.

Le volume racine de remplacement a les mêmes attributs de type, de taille et de suppression à la résiliation que le volume racine d'origine.

Remplacement d'un volume racine à l'aide d'un instantané

Vous pouvez procéder à un remplacement de volume racine qui consiste à remplacer le volume racine d'une instance par un volume de remplacement restauré sur un instantané spécifique. Cela vous permet de restaurer le volume racine d'une instance à un instantané spécifique que vous avez précédemment créé à partir de ce volume racine.

Le volume racine de remplacement a les mêmes attributs de type, de taille et de suppression à la résiliation que le volume racine d'origine.

Considérations relatives à l'utilisation d'un instantané

- Vous ne pouvez utiliser que des instantanés appartenant à la même lignée que le volume racine actuel de l'instance.
- Vous ne pouvez pas utiliser de copies d'instantanés créées à partir d'instantanés provenant du volume racine.
- Après avoir remplacé avec succès le volume racine, les instantanés pris à partir du volume racine d'origine peuvent encore être utilisés pour remplacer le nouveau volume racine (de remplacement).

Remplacement d'un volume racine à l'aide d'une AMI

Vous pouvez effectuer un remplacement de volume racine à l'aide d'une AMI que vous possédez ou d'une AMI partagée avec vous. L'AMI doit avoir le même code produit, les mêmes informations de facturation, le même type d'architecture et le même type de virtualisation que l'instance.

Si l'instance est activée pour ENA ou sriov-net, vous devez utiliser une AMI compatible avec ces fonctionnalités. Si l'instance n'est pas activée pour ENA ou sriov-net, vous pouvez soit sélectionner une AMI qui ne prend pas en charge ces fonctionnalités, soit ajouter automatiquement une prise en charge si vous sélectionnez une AMI compatible avec ENA ou sriov-net.

Si l'instance est activée pour NitroTPM, vous devez utiliser une AMI sur laquelle NitroTPM est activé. Le support NitroTPM n'est pas activé si l'instance n'a pas été configurée pour cela, quelle que soit l'AMI que vous sélectionnez.

Vous pouvez sélectionner une AMI avec un mode de démarrage différent de celui de l'instance, à condition que l'instance prenne en charge le mode de démarrage de l'AMI. Si l'instance ne prend pas en charge le mode de démarrage, la demande échoue. Si l'instance prend en charge le mode de démarrage, le nouveau mode de démarrage est propagé à l'instance et ses données UEFI sont mises à jour en conséquence. Si vous avez modifié manuellement l'ordre de démarrage ou ajouté une clé privée UEFI Secure Boot pour charger des modules de noyau privés, les modifications sont perdues lors du remplacement du volume racine.

Le volume racine de remplacement reçoit les mêmes attributs de volume, de type et de suppression à la résiliation que le volume racine d'origine et il obtient la taille du mappage de périphérique de stockage en mode bloc du volume racine de l'AMI.

Note

La taille du mappage de périphérique de stockage en mode bloc du volume racine de l'AMI doit être égale ou supérieure à la taille du volume racine d'origine. Si la taille du mappage de périphérique de stockage en mode bloc du volume racine de l'AMI est inférieure à la taille du volume racine d'origine, la demande échoue.

Une fois la tâche de remplacement du volume racine terminée, les informations nouvelles et mises à jour suivantes sont reflétées lorsque vous décrivez l'instance à l'aide de la console AWS CLI ou AWS des SDK :

- Nouvel ID d'AMI
- Nouvel ID de volume pour le volume racine
- Mise à jour de la configuration du mode de démarrage (si elle est modifiée par l'AMI)
- Mise à jour de la configuration de NitroTPM (si elle est activée par l'AMI)

- Mise à jour de la configuration d'ENA (si elle est activée par l'AMI)
- Mise à jour de la configuration de sriov-net (si elle est activée par l'AMI)

Le nouvel ID d'AMI est également reflété dans les métadonnées de l'instance.

Considérations relatives à l'utilisation d'une AMI :

- Si vous utilisez une AMI comportant plusieurs mappages de périphérique de stockage en mode bloc, seul le volume racine de l'AMI est utilisé. Les autres volumes (non racine) sont ignorés.
- Vous ne pouvez utiliser cette fonction que si vous disposez d'autorisations sur l'AMI et sur l'instantané du volume racine qui lui est associé. Vous ne pouvez pas utiliser cette fonctionnalité avec les AWS Marketplace AMI.
- Vous pouvez seulement utiliser une AMI sans code produit si l'instance n'a pas de code produit.
- La taille du mappage de périphérique de stockage en mode bloc du volume racine de l'AMI doit être égale ou supérieure à la taille du volume racine d'origine. Si la taille du mappage de périphérique de stockage en mode bloc du volume racine de l'AMI est inférieure à la taille du volume racine d'origine, la demande échoue.
- Les documents d'identité de l'instance sont automatiquement mis à jour.
- Si l'instance prend en charge NitroTPM, les données NitroTPM de l'instance sont réinitialisées et de nouvelles clés sont générées.

Remplacer un volume racine

Lorsque vous remplacez le volume racine d'une instance, une tâche de remplacement du volume racine est créé. Vous pouvez utiliser la tâche de remplacement du volume racine pour surveiller la progression et le résultat du processus de remplacement. Pour plus d'informations, consultez [Afficher les tâches de remplacement du volume racine](#).

Vous pouvez remplacer le volume racine d'une instance à l'aide d'une des méthodes suivantes.

Note

Si vous utilisez la console Amazon EC2, notez que cette fonctionnalité n'est disponible que dans la nouvelle console.

New console

Pour remplacer le volume racine

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance dont vous souhaitez remplacer le volume racine et choisissez Actions, Surveiller et résoudre les problèmes, Remplacer le volume racine.

Note

L'action Replace root volume (Remplacer le volume racine) est désactivée si l'instance sélectionnée n'est pas dans l'état `running`.

4. Dans l'écran Remplacer le volume racine, effectuez l'une des opérations suivantes :
 - Pour restaurer le volume racine de remplacement à son état de lancement initial, choisissez Create replacement task (Créer une tâche de remplacement) sans sélectionner d'instantané.
 - Pour restaurer le volume racine de remplacement à un instantané spécifique, pour Snapshot (Instantané), sélectionnez l'instantané à utiliser, puis choisissez Create replacement task (Créer une tâche de remplacement).
 - Pour restaurer le volume racine de remplacement à l'aide d'une AMI, pour AMI, sélectionnez l'AMI à utiliser, puis choisissez Create replacement task (Créer une tâche de remplacement).
5. Pour supprimer le volume racine d'origine une fois la tâche de remplacement terminée, sélectionnez Delete replaced root volume (Supprimer le volume racine remplacé).

AWS CLI

Pour restaurer le volume racine de remplacement à l'état de lancement

Utilisez la commande [create-replace-root-volume-task](#). Pour `--instance-id`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Omettez les paramètres `--snapshot-id` et `--image-id`. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `--delete-replaced-root-volume` et spécifiez `true`.

```
$ aws ec2 create-replace-root-volume-task \
```

```
--instance-id i-1234567890abcdef0 \  
--delete-replaced-root-volume true
```

Pour restaurer le volume racine de remplacement à un instantané spécifique

Utilisez la commande [create-replace-root-volume-task](#). Pour `--instance-id`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Pour `--snapshot-id`, spécifiez l'ID de l'instantané à utiliser. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `--delete-replaced-root-volume` et spécifiez `true`.

```
$ aws ec2 create-replace-root-volume-task \  
--instance-id i-1234567890abcdef0 \  
--snapshot-id snap-9876543210abcdef0 \  
--delete-replaced-root-volume true
```

Pour restaurer le volume racine de remplacement à l'aide d'une AMI

Utilisez la commande [create-replace-root-volume-task](#). Pour `--instance-id`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Pour `--image-id`, spécifiez l'ID de l'AMI à utiliser. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `--delete-replaced-root-volume` et spécifiez `true`.

```
$ aws ec2 create-replace-root-volume-task \  
--instance-id i-01234567890abcdef \  
--image-id ami-09876543210abcdef \  
--delete-replaced-root-volume true
```

Tools for Windows PowerShell

Pour restaurer le volume racine de remplacement à l'état de lancement

Utilisez la commande [New-EC2ReplaceRootVolumeTask](#). Pour `-InstanceId`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Omettez les paramètres `-SnapshotId` et `-ImageId`. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `-DeleteReplacedRootVolume` et spécifiez `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -  
DeleteReplacedRootVolume $true
```

Pour restaurer le volume racine de remplacement à un instantané spécifique

Utilisez la commande [New-EC2ReplaceRootVolumeTask](#). Pour `--InstanceId`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Pour `-SnapshotId`, spécifiez l'ID de l'instantané à utiliser. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `-DeleteReplacedRootVolume` et spécifiez `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -  
SnapshotId snap-9876543210abcdef0 -DeleteReplacedRootVolume $true
```

Pour restaurer le volume racine de remplacement à l'aide d'une AMI

Utilisez la commande [New-EC2ReplaceRootVolumeTask](#). Pour `-InstanceId`, spécifiez l'ID de l'instance dont le volume racine doit être remplacé. Pour `-ImageId`, spécifiez l'ID de l'AMI à utiliser. Pour supprimer le volume racine d'origine après qu'il ait été remplacé, incluez `-DeleteReplacedRootVolume` et spécifiez `$true`.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -  
ImageId ami-09876543210abcdef -DeleteReplacedRootVolume $true
```

Afficher les tâches de remplacement du volume racine

Lorsque vous remplacez le volume racine d'une instance, une tâche de remplacement du volume racine est créée. La tâche de remplacement du volume racine passe par les états suivants pendant le processus :

- `pending` — Le volume de remplacement est en cours de création.
- `in-progress` — Le volume d'origine est en cours de détachement, tandis que le volume de remplacement est en cours d'attachement.
- `succeeded` — Le volume de remplacement a été attaché à l'instance et celle-ci est disponible.
- `failing` — La tâche de remplacement est en train d'échouer.
- `failed` — La tâche de remplacement a échoué, mais le volume racine d'origine est toujours attaché.
- `failing-detached` — La tâche de remplacement est en train d'échouer et il est possible que l'instance n'ait pas de volume racine attaché.
- `failed-detached` — La tâche de remplacement a échoué et l'instance n'a pas de volume racine attaché.

Vous pouvez afficher les tâches de remplacement du volume racine d'une instance à l'aide d'une des méthodes suivantes.

Note

Si vous utilisez la console Amazon EC2, notez que cette fonctionnalité n'est disponible que dans la nouvelle console.

Console

Pour afficher les tâches de remplacement du volume racine

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance dont vous souhaitez afficher les tâches de remplacement du volume racine, puis choisissez l'onglet Stockage.
4. Sous l'onglet Stockage, développez Récentes tâches de remplacement du volume racine.

AWS CLI

Pour afficher l'état d'une tâche de remplacement du volume racine

Utilisez la commande [describe-replace-root-volume-tasks](#) (Décrire les tâches de remplacement du volume racine) et spécifiez les ID des tâches de remplacement du volume racine à afficher.

```
$ aws ec2 describe-replace-root-volume-tasks \
--replace-root-volume-task-ids replacevol-1234567890abcdef0
```

```
{
  "ReplaceRootVolumeTasks": [
    {
      "ReplaceRootVolumeTaskId": "replacevol-1234567890abcdef0",
      "InstanceId": "i-1234567890abcdef0",
      "TaskState": "succeeded",
      "StartTime": "2020-11-06 13:09:54.0",
      "CompleteTime": "2020-11-06 13:10:14.0",
      "SnapshotId": "snap-01234567890abcdef",
      "DeleteReplacedRootVolume": "True"
    }
  ]
}
```

```
}]  
}
```

Vous pouvez également utiliser le filtre `instance-id` pour filtrer les résultats par instance.

```
$ aws ec2 describe-replace-root-volume-tasks \  
--filters Name=instance-id,Values=i-1234567890abcdef0
```

Tools for Windows PowerShell

Pour afficher l'état d'une tâche de remplacement du volume racine

Utilisez la [Get-EC2ReplaceRootVolumeTask](#) commande et spécifiez les identifiants des tâches de remplacement du volume racine à afficher.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -  
ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0
```

Vous pouvez également utiliser le filtre `instance-id` pour filtrer les résultats par instance.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =  
'i-1234567890abcdef0'} | Format-Table
```

Noms des appareils sur les instances Amazon EC2

Lorsque vous associez un volume à votre instance, vous incluez un nom d'appareil pour le volume. Ce nom d'appareil est utilisé par Amazon EC2. Le pilote du périphérique de stockage en mode bloc de l'instance attribue le nom réel du volume au montage de celui-ci et le nom affecté peut être différent de celui recommandé par Amazon EC2.

Le nombre maximum de volumes que votre instance peut prendre en charge dépend du système d'exploitation. Pour plus d'informations, consultez [Limites de volume d'instance](#).

Table des matières

- [Noms d'appareil disponibles](#)
- [Considérations sur les noms d'appareil](#)

Noms d'appareil disponibles

Instances Linux

Deux types de virtualisation sont disponibles pour les instances Linux : la virtualisation paravirtuelle (PV) et la virtualisation HVM. Le type de virtualisation d'une instance est déterminé par l'AMI utilisée pour lancer cette instance. Tous les types d'instance prennent en charge les AMI HVM. Certains types d'instance de la génération précédente prennent en charge les AMI PV. Veillez à noter le type de virtualisation de votre AMI dans la mesure où les noms d'appareil recommandés et disponibles que vous utilisez dépendent du type de virtualisation de votre instance. Pour plus d'informations, consultez [Types de virtualisation AMI](#).

Le tableau ci-après répertorie les noms d'appareils disponibles que vous pouvez spécifier dans un mappage de périphérique de stockage en mode bloc ou lorsque vous attachez un volume EBS.

Type de virtualisation	Disponible	Réservé pour le volume racine	Recommandé pour les volumes EBS	Volumes de stockage d'instance
Paravirtuel	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
HVM	/dev/sd[a-z] /dev/xvd[a-d][a-z] /dev/xvd[e-z]	Diffère selon l'AMI /dev/sda1 or /dev/xvda	/dev/sd[f-p] *	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge)

Type de virtualisation	Disponible	Réservé pour le volume racine	Recommandé pour les volumes EBS	Volumes de stockage d'instance
				**

* Les noms d'appareil que vous spécifiez pour les volumes EBS NVMe dans un mappage de périphérique de stockage en mode bloc sont remplacés par les noms du périphérique NVMe (/dev/nvme[0-26]n1). Le pilote du périphérique de stockage en mode bloc peut attribuer les noms de périphériques NVMe dans un autre ordre que celui que vous avez spécifié pour les volumes dans le mappage de périphériques de stockage en mode bloc.

** Les volumes de stockage d'instance NVMe sont automatiquement énumérés et un nom d'appareil NVMe leur est automatiquement attribué.

instances Windows

Les AMI Windows utilisent l'un des ensembles de pilotes suivants pour autoriser l'accès au matériel virtualisé : AWS PV, Citrix PV et RedHat PV. Pour plus d'informations, consultez [the section called "Pilotes PV pour Windows"](#).

Le tableau ci-après répertorie les noms d'appareils disponibles que vous pouvez spécifier dans un mappage de périphérique de stockage en mode bloc ou lorsque vous attachez un volume EBS.

Type de pilote	Disponible	Réservé pour le volume racine	Recommandé pour les volumes EBS	Volumes de stockage d'instances
AWS PV, Citrix PV	xvd[b-z]	/dev/sda1	xvd[f-z] *	xvdc[a-x]
	xvd[b-c][a-z]			xvd[a-e]
	/dev/sda1			**
	/dev/sd[b-e]			
Virtualisation paravirtuelle Red Hat	xvd[a-z]	/dev/sda1	xvd[f-p]	xvdc[a-x]
	xvd[b-c][a-z]			xvd[a-e]

Type de pilote	Disponible	Réservé pour le volume racine	Recommandé pour les volumes EBS	Volumes de stockage d'instances
	/dev/sda1			
	/dev/sd[b-e]			

* Pour Citrix PV et Red Hat PV, si vous mappez un volume EBS avec son nom xvda, Windows ne reconnaît pas le volume (le volume est visible pour AWS PV ou AWS NVMe).

** Les volumes de stockage d'instance NVMe sont automatiquement énumérés et une lettre de lecteur Windows leur est automatiquement attribuée.

Pour plus d'informations sur les volumes de stockage d'instance, consultez [Stockage d'instances Amazon EC2](#). Pour plus d'informations sur les volumes NVMe EBS (instances basées sur Nitro), notamment sur la façon d'identifier le périphérique EBS, consultez Amazon EBS et [NVMe dans le guide de l'utilisateur Amazon EBS](#).

Considérations sur les noms d'appareil

Gardez les points suivants à l'esprit lorsque vous sélectionnez un nom d'appareil :

- Bien que vous puissiez relier vos volumes EBS à l'aide des noms d'appareil utilisés pour relier les volumes de stockage d'instances, nous vous recommandons fortement de ne pas le faire dans la mesure où les résultats peuvent être imprévisibles.
- Le nombre de volumes de stockage d'instance NVMe pour une instance dépend de la taille de cette dernière. Les volumes de stockage d'instance NVMe sont automatiquement énumérés et on leur attribue un nom de périphérique NVMe (instances Linux) ou une lettre de lecteur Windows (instances Windows).
- (Instances Windows) Les AMI AWS Windows sont fournies avec un logiciel supplémentaire qui prépare une instance lors de son premier démarrage. Il s'agit du service EC2Config (AMI Windows antérieures à Windows Server 2016) ou EC2Launch (Windows Server 2016 et versions ultérieures). Une fois que les appareils ont été mappés aux lecteurs, ils sont initialisés et montés. Le lecteur racine est initialisé et monté en tant que C:\. Par défaut, lorsqu'un volume EBS est attaché à une instance Windows, il peut être représenté par n'importe quelle lettre de lecteur sur l'instance. Vous pouvez modifier les paramètres afin de définir les lettres de lecteur des volumes EBS selon vos spécifications. Par exemple, les volumes de stockage, la valeur par

défaut dépend du pilote. AWS Les pilotes PV et Citrix PV attribuent aux volumes de stockage des instances des lettres de lecteur allant de Z : à A :. Les pilotes Red Hat attribuent les lettres de lecteurs de volumes de stockage d'instances allant de D: à A:. Pour plus d'informations, consultez [Configuration des paramètres de lancement pour les instances Windows Amazon EC2](#) et [Mapper des disques sur des volumes sur votre instance Windows](#).

- (Instances Linux) Selon le pilote de périphérique en mode bloc du noyau, le périphérique peut être attaché sous un nom différent de celui que vous avez spécifié. Par exemple, si vous spécifiez un nom de périphérique de `/dev/sdh`, votre appareil peut être renommé `/dev/xvdh` ou `/dev/hdh`. Dans la plupart des cas, la lettre finale reste la même. Dans certaines versions de Red Hat Enterprise Linux (et ses variantes, telles que CentOS), la lettre finale peut changer (`/dev/sda` peut devenir `/dev/xvde`). Dans ces cas, la lettre finale de chaque nom de périphérique est incrémentée le même nombre de fois. Par exemple, si `/dev/sdb` est renommé `/dev/xvdf`, alors `/dev/sdc` est renommé `/dev/xvdg`. Amazon Linux crée un lien symbolique pour le nom que vous avez spécifié pour le périphérique renommé. D'autres systèmes d'exploitation peuvent avoir un comportement différent.
- (Instances Linux) Les AMI HVM ne prennent pas en charge l'utilisation de numéros de fin sur les noms des appareils, à l'exception de `/dev/sda1`, qui est réservé au périphérique racine, et `/dev/sda2`. L'utilisation de `/dev/sda2` est possible, mais nous ne recommandons pas l'utilisation de ce mappage de périphérique avec les instances HVM.
- (Instances Linux) Lorsque vous utilisez des AMI PV, vous ne pouvez pas associer de volumes qui partagent les mêmes lettres de périphérique, avec ou sans chiffres de fin. Par exemple, si vous attachez un premier volume en tant que `/dev/sdc` et un autre volume en tant que `/dev/sdc1`, seul `/dev/sdc` sera visible pour l'instance. Pour utiliser des chiffres à la fin des noms de périphériques, vous devez y avoir recours pour tous les noms de périphériques qui partagent les mêmes lettres de base (par exemple `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- (Instances Linux) Certains noyaux personnalisés peuvent comporter des restrictions qui limitent leur utilisation à `/dev/sd[f-p]` ou `/dev/sd[f-p][1-6]`. Si vous rencontrez des difficultés en utilisant `/dev/sd[q-z]` ou `/dev/sd[q-z][1-6]`, essayez avec `/dev/sd[f-p]` ou `/dev/sd[f-p][1-6]`.

Avant de spécifier le nom de l'appareil que vous avez sélectionné, vérifiez qu'il est disponible. Sinon, vous recevrez un message d'erreur indiquant que le nom de l'appareil est déjà utilisé. Pour afficher les unités de disque et leurs points de montage, utilisez la `lsblk` commande (instances Linux), l'utilitaire de gestion des disques ou la `diskpart` commande (instances Windows).

Mappages de périphériques de stockage en mode bloc

Chaque instance que vous lancez comporte un volume de périphérique racine associé, qui correspond à un volume Amazon EBS ou à un volume de stockage d'instance. Vous pouvez utiliser un mappage de périphérique de stockage en mode bloc pour spécifier des volumes EBS supplémentaires ou des volumes de stockage d'instance à attacher à une instance lorsqu'elle est lancée. Vous pouvez également associer des volumes EBS supplémentaires à une instance en cours d'exécution. Cependant, le seul moyen d'attacher des volumes de stockage d'instance à une instance est d'utiliser le mappage de périphérique de stockage en mode bloc pour les attacher lors du lancement de l'instance.

Table des matières

- [Concepts de mappage de périphérique de stockage en mode bloc](#)
- [Mappage de périphérique de stockage en mode bloc d'une AMI](#)
- [Mappage de périphérique de stockage en mode bloc d'une instance](#)

Concepts de mappage de périphérique de stockage en mode bloc

Un périphérique de stockage en mode bloc est un dispositif de stockage qui déplace des données en séquence d'octets ou bits (blocs). Ces dispositifs prennent en charge l'accès aléatoire et utilisent généralement des I/O mises en mémoire tampon. Ce sont par exemple des disques durs, des lecteurs de CD-ROM et des lecteurs flash. Un périphérique de stockage en mode bloc peut être physiquement attaché à un ordinateur ou accessible à distance comme s'il était physiquement attaché à l'ordinateur.

Amazon EC2 prend en charge deux types de périphériques de stockage en mode bloc :

- Les volumes de stockage d'instance (périphériques virtuels dont le matériel sous-jacent est physiquement attaché à l'ordinateur hôte de l'instance)
- Les volumes EBS (périphériques de stockage à distance)

Un mappage de périphérique de stockage en mode bloc définit les périphériques de stockage en mode bloc (volumes de stockage d'instance et volumes EBS) qui doivent être attachés à l'instance. Vous pouvez spécifier un mappage de périphérique de stockage en mode bloc lors de la création d'une AMI, afin que le mappage soit utilisé par toutes les instances lancées à partir de l'AMI. Vous pouvez également spécifier un mappage de périphérique de stockage en mode bloc lorsque vous

lancez une instance, afin que son mappage remplace celui spécifié dans l'AMI à partir de laquelle vous avez lancé l'instance. Notez que tous les volumes de stockage d'instance NVMe pris en charge par un type d'instance sont automatiquement énumérés et un nom de périphérique leur est automatiquement attribué au lancement de l'instance. Le fait de les ajouter dans votre mappage de périphérique de stockage en mode bloc n'a aucun effet.

Sommaire

- [Entrées du mappage de périphérique de stockage en mode bloc](#)
- [Mises en garde sur le stockage d'instance du mappage de périphérique de stockage en mode bloc](#)
- [Exemple de mappage de périphérique de stockage en mode bloc](#)
- [Mise à disposition d'appareils dans le système d'exploitation](#)

Entrées du mappage de périphérique de stockage en mode bloc

Lorsque vous créez un mappage de périphérique de stockage en mode bloc, vous spécifiez les informations suivantes pour chaque périphérique de stockage en mode bloc qui doit être attaché à l'instance :

- Le nom du périphérique utilisé dans Amazon EC2. Le pilote du périphérique de stockage en mode bloc de l'instance attribue le nom de volume réel lors du montage du volume. Le nom attribué peut être différent de celui recommandé par Amazon EC2. Pour plus d'informations, consultez [Noms des appareils sur les instances Amazon EC2](#).

Pour les volumes de stockage d'instance, vous spécifiez également les informations suivantes :

- Le nom du périphérique virtuel : `ephemeral[0-23]`. Notez que le nombre et la taille des volumes de stockage d'instance disponibles pour votre instance varient en fonction du type d'instance.

Pour les volumes de stockage d'instance NVMe, les informations suivantes s'appliquent également :

- Ces volumes sont automatiquement énumérés et un nom de périphérique leur est automatiquement attribué. Le fait de les ajouter dans votre mappage de périphérique de stockage en mode bloc n'a aucun effet.

Pour les volumes EBS, vous spécifiez également les informations suivantes :

- L'ID de l'instantané à utiliser pour créer le périphérique de stockage en mode bloc (snap-xxxxxxx). Cette valeur est facultative si vous spécifiez une taille de volume. Vous ne pouvez pas spécifier l'ID d'instantané archivé.
- Taille du volume en Gio La taille spécifiée doit être supérieure ou égale à la taille de l'instantané spécifié.
- Suppression ou non du volume lors de l'arrêt de l'instance (`true` ou `false`). La valeur par défaut est `true` pour le volume du périphérique racine et `false` pour les volumes attachés. Lorsque vous créez une AMI, son mappage de périphérique de stockage en mode bloc hérite de ce paramètre de l'instance. Lorsque vous lancez une instance, elle hérite de ce paramètre de l'AMI.
- Le type de volume, qui peut être `gp2` et `gp3` pour les SSD à usage général, `io1` et `io2` pour les SSD IOPS provisionnés, `st1` pour les HDD à débit optimisé, `sc1` pour les HDD à froid ou `standard` pour les volumes magnétiques.
- Le nombre d'opérations d'IOPS (IOPS) prises en charge par le volume. (Utilisé uniquement avec les volumes `io1` et `io2`.)

Mises en garde sur le stockage d'instance du mappage de périphérique de stockage en mode bloc

Vous devez prendre en compte plusieurs mises en garde lorsque vous lancez des instances avec des AMIs comportant des volumes de stockage d'instance dans leurs mappages de périphérique de stockage en mode bloc.

- Certains types d'instance comprennent un plus grand nombre de volumes de stockage d'instance que d'autres et certains types d'instance ne contiennent aucun volume de stockage d'instance. Si votre type d'instance prend en charge un volume de stockage d'instance et que votre AMI comporte des mappages pour deux volumes de stockage d'instance, l'instance est lancée avec un volume de stockage d'instance.
- Les volumes de stockage d'instance peuvent uniquement être mappés au moment du lancement. Vous ne pouvez pas arrêter une instance sans volume de stockage d'instance (comme `t2.micro`), modifier le type de l'instance par un type prenant en charge les volumes de stockage d'instance, puis redémarrer l'instance avec des volumes de stockage d'instance. En revanche, vous pouvez créer une AMI à partir de l'instance et la lancer sur un type d'instance prenant en charge les volumes de stockage d'instance, et mapper ces volumes de stockage d'instance à l'instance.

- Si vous lancez une instance à laquelle sont mappés des volumes de stockage d'instance, puis arrêtez l'instance, en modifiez le type avec un nombre inférieur de volumes de stockage d'instance et redémarrez l'instance, les mappages des volumes de stockage d'instance du lancement initial apparaissent toujours dans les métadonnées de l'instance. Cependant, l'instance n'a accès qu'au nombre maximum de volumes de stockage d'instance pris en charge pour ce type d'instance.

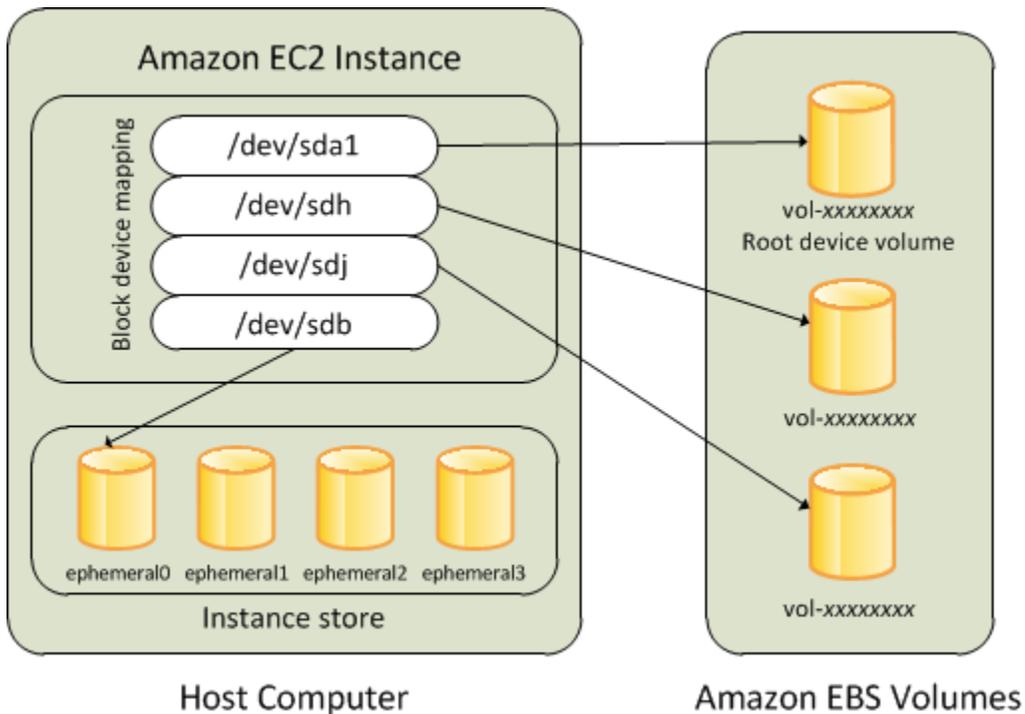
Note

Lorsqu'une instance est arrêtée, toutes les données stockées sur les volumes de stockage d'instance sont perdues.

- En fonction de la capacité de stockage de l'instance au moment du lancement, les instances M3 peuvent ignorer les mappages de périphérique de stockage en mode bloc du stockage d'instance AMI au moment du lancement, sauf s'ils sont spécifiés au moment du lancement. Il est conseillé de spécifier les mappages de périphérique de stockage en mode bloc du stockage d'instance au moment du lancement, même si les volumes d'instance de stockage de l'AMI que vous lancez sont mappés dans l'AMI, afin de garantir la disponibilité des volumes de stockage d'instance au lancement de l'instance.

Exemple de mappage de périphérique de stockage en mode bloc

L'illustration suivante montre un exemple de mappage de périphérique de stockage en mode bloc pour une instance basée sur les volumes EBS. `/dev/sdb` est mappé à `ephemeral0` et deux volumes EBS sont mappés. L'un à `/dev/sdh` et l'autre à `/dev/sdj`. La figure illustre également le volume EBS qui est le volume du périphérique racine, `/dev/sda1`.



Notez que cet exemple de mappage de périphérique de stockage en mode bloc est utilisé dans les exemples de commandes et d'API de cette rubrique. Les exemples de commandes et d'API qui créent les mappages de périphérique de stockage en mode bloc sont disponibles dans les sections [Spécifier un mappage de périphérique de stockage en mode bloc pour une AMI](#) et [Mettre à jour le mappage de périphérique de stockage en mode bloc lors du lancement d'une instance](#).

Mise à disposition d'appareils dans le système d'exploitation

Les noms de périphériques tels que `/dev/sdh` et `xvdh` sont utilisés par Amazon EC2 pour décrire des périphériques de stockage en mode bloc. Le mappage de périphérique de stockage en mode bloc est utilisé par Amazon EC2 pour spécifier les périphériques de stockage en mode bloc qui doivent être attachés à une instance EC2. Lorsqu'un périphérique de stockage en mode bloc est attaché à une instance, il doit être monté par le système d'exploitation pour que vous puissiez accéder au dispositif de stockage. Lorsqu'un périphérique de stockage en mode bloc est détaché d'une instance, il doit être démonté par le système d'exploitation. Ainsi, vous ne pouvez plus accéder au dispositif de stockage.

Instances Linux : les noms des périphériques spécifiés dans le mappage des périphériques par blocs sont mappés aux périphériques par blocs correspondants lors du premier démarrage de l'instance. Le type d'instance détermine les volumes de stockage d'instance qui sont formatés et montés par défaut. Vous pouvez monter des volumes de stockage d'instance supplémentaires au moment du lancement, à condition de ne pas dépasser le nombre de volumes de stockage d'instance disponibles

pour votre type d'instance. Pour plus d'informations, consultez [Stockage d'instances Amazon EC2](#). Le pilote du périphérique de stockage en mode bloc pour l'instance détermine les périphériques utilisés lorsque les volumes sont formatés et montés.

Instances Windows : les noms des périphériques spécifiés dans le mappage des périphériques par blocs sont mappés aux périphériques par blocs correspondants lorsque l'instance démarre pour la première fois, puis le service Ec2Config initialise et monte les lecteurs. Le volume du périphérique racine est monté en tant que C:\. Les volumes de stockage d'instance sont montés en tant que Z:\, Y:\, etc. Le montage d'un volume EBS peut être effectué à l'aide de n'importe quelle lettre de lecteur disponible. Vous pouvez toutefois configurer la manière dont les lettres de lecteur sont attribuées aux volumes EBS ; pour plus d'informations, consultez [the section called "Configuration des agents de lancement Windows"](#).

Mappage de périphérique de stockage en mode bloc d'une AMI

Chaque AMI comporte un mappage de périphérique de stockage en mode bloc qui spécifie les périphériques de stockage en mode bloc à attacher à une instance lancée à partir de l'AMI. Pour ajouter d'autres périphériques de stockage en mode bloc à une AMI, vous devez créer votre propre AMI.

Sommaire

- [Spécifier un mappage de périphérique de stockage en mode bloc pour une AMI](#)
- [Afficher les volumes EBS dans un mappage de périphérique de stockage en mode bloc d'une AMI](#)

Spécifier un mappage de périphérique de stockage en mode bloc pour une AMI

Lorsque vous créez une AMI, il existe deux façons de spécifier des volumes en plus du volume racine. Si vous avez déjà attaché des volumes à une instance en cours d'exécution avant de créer une AMI à partir de l'instance, le mappage de périphérique de stockage en mode bloc pour l'AMI comprend ces mêmes volumes. Pour les volumes EBS, les données existantes sont enregistrées dans un nouvel instantané. C'est ce nouvel instantané qui est spécifié dans le mappage de périphérique de stockage en mode bloc. Pour les volumes de stockage d'instance, les données ne sont pas conservées.

Pour une AMI basée sur des volumes EBS, vous pouvez ajouter des volumes EBS et des volumes de stockage d'instance à l'aide d'un mappage de périphérique de stockage en mode bloc. Pour une AMI basée sur le stockage d'instance, vous pouvez ajouter des volumes de stockage d'instance

uniquement en modifiant les entrées du mappage de périphérique de stockage en mode bloc dans le fichier manifest des images lors de l'enregistrement de l'image.

Note

Pour les instances M3, vous devez spécifier les volumes de stockage d'instance dans le mappage de périphérique de stockage en mode bloc de l'instance lorsque cette dernière est lancée. Lorsque vous lancez une instance M3, les volumes de stockage d'instance spécifiés dans le mappage de périphérique de stockage en mode bloc de l'AMI peuvent être ignorés s'ils ne sont pas spécifiés dans le cadre du mappage de périphérique de stockage en mode bloc de l'instance.

Console

Pour ajouter des volumes à une AMI à l'aide de la console

1. Ouvrez la console Amazon EC2.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez une instance, puis Actions, Image and templates (Image et modèles), Create image (Créer une image).
4. Saisissez un nom et une description pour l'image.
5. Les volumes d'instance apparaissent sous Instance volumes (Volumes d'instance). Pour ajouter un autre volume, sélectionnez Add volume (Ajouter un volume).
6. Pour Volume type (Type de volume), sélectionnez le type de volume. Pour Device (Périphérique), sélectionnez le nom du périphérique. Pour un volume EBS, vous pouvez spécifier des informations supplémentaires, telles qu'un instantané, la taille du volume, le type de volume, les IOPS et l'état de chiffrement.
7. Choisissez Create image (Créer une image).

Command line

Pour ajouter des volumes à une AMI à l'aide de la ligne de commande

Utilisez la AWS CLI commande [create-image](#) pour spécifier un mappage de périphériques en mode bloc pour une AMI basée sur EBS. Utilisez la AWS CLI commande [register-image](#) pour

spécifier un mappage de périphériques en mode bloc pour une AMI basée sur une instance store-backed.

Spécifiez le mappage de périphérique de stockage en mode bloc à l'aide du paramètre `--block-device-mappings`. Les arguments encodés en JSON peuvent être fournis soit directement depuis la ligne de commande soit par référence à un fichier :

```
--block-device-mappings [mapping, ...]  
--block-device-mappings [file://mapping.json]
```

Pour ajouter un volume de stockage d'instance, utilisez le mappage suivant :

```
{  
  "DeviceName": "device_name",  
  "VirtualName": "ephemeral0"  
}
```

Pour ajouter un volume gp2 vide de 100 Gio, utilisez le mappage suivant :

```
{  
  "DeviceName": "device_name",  
  "Ebs": {  
    "VolumeSize": 100  
  }  
}
```

Pour ajouter un volume EBS basé sur un instantané, utilisez le mappage suivant :

```
{  
  "DeviceName": "device_name",  
  "Ebs": {  
    "SnapshotId": "snap-xxxxxxxx"  
  }  
}
```

Pour omettre un mappage pour un périphérique, utilisez le mappage suivant :

```
{  
  "DeviceName": "device_name",  
  "NoDevice": ""  
}
```

```
}
```

Vous pouvez aussi utiliser le paramètre `-BlockDeviceMapping` avec les commandes suivantes (AWS Tools for Windows PowerShell) :

- [New-EC2Image](#)
- [Register-EC2Image](#)

Afficher les volumes EBS dans un mappage de périphérique de stockage en mode bloc d'une AMI

Vous pouvez facilement énumérer les volumes EBS du mappage de périphérique de stockage en mode bloc pour une AMI.

Console

Pour afficher les volumes EBS pour une AMI à l'aide de la console

1. Ouvrez la console Amazon EC2.
2. Dans le panneau de navigation, sélectionnez AMI.
3. Choisissez EBS images dans la liste Filter pour obtenir la liste des AMI basées sur EBS.
4. Sélectionnez l'AMI souhaitée et consultez l'onglet Details. Au minimum, les informations suivantes sont disponibles pour le périphérique racine :
 - Type de périphérique racine (ebs)
 - Nom du périphérique racine (par exemple, `/dev/sda1`)
 - Block Devices (par exemple, `/dev/sda1=snap-1234567890abcdef0:8:true`)

Si l'AMI a été créée avec des volumes EBS supplémentaires à l'aide d'un mappage de périphérique de stockage en mode bloc, le champ Block Devices affiche également le mappage pour ces volumes supplémentaires. Notez que cet écran n'affiche pas les volumes de stockage d'instance.

Command line

Pour afficher les volumes EBS d'une AMI à l'aide de la ligne de commande

Utilisez la commande [describe-images](#) (AWS CLI) ou la commande [Get-EC2Image](#) (AWS Tools for Windows PowerShell) pour énumérer les volumes EBS dans le mappage de périphériques en mode bloc pour une AMI.

Mappage de périphérique de stockage en mode bloc d'une instance

Par défaut, une instance que vous lancez comprend tous les périphériques de stockage spécifiés dans le mappage de périphérique de stockage en mode bloc de l'AMI à partir de laquelle vous avez lancé l'instance. Vous pouvez spécifier les modifications apportées au mappage de périphérique de stockage en mode bloc d'une instance lorsque vous la lancez. Ces mises à jour remplacent le mappage de périphérique de stockage en mode bloc de l'AMI ou fusionnent avec.

Limites

- Pour le volume racine, vous pouvez uniquement modifier les données informations suivantes : taille du volume, type de volume et indicateur Delete on Termination.
- Lorsque vous modifiez un volume EBS, vous ne pouvez pas en diminuer la taille. Vous devez donc spécifier un instantané dont la taille est égale ou supérieure à celle de l'instantané spécifié dans le mappage de périphérique de stockage en mode bloc de l'AMI.

Sommaire

- [Mettre à jour le mappage de périphérique de stockage en mode bloc lors du lancement d'une instance](#)
- [Mettre à jour le mappage de périphérique de stockage en mode bloc d'une instance en cours d'exécution](#)
- [Afficher les volumes EBS dans le mappage de périphérique de stockage en mode bloc d'une instance](#)
- [Afficher le mappage de périphérique de stockage en mode bloc d'une instance pour les volumes de stockage d'instances](#)

Mettre à jour le mappage de périphérique de stockage en mode bloc lors du lancement d'une instance

Vous pouvez ajouter des volumes EBS et des volumes de stockage d'instance à une instance lors de son lancement. Notez que la mise à jour du mappage de périphérique de stockage en mode bloc

d'une instance n'entraîne pas de modification permanente du mappage de périphérique de stockage en mode bloc de l'AMI à partir de laquelle il a été lancé.

Console

Pour ajouter des volumes à une instance à l'aide de la console

1. Ouvrez la console Amazon EC2.
2. Sur le tableau de bord, choisissez Lancer une instance.
3. Sur la page Choose an Amazon Machine Image (AMI), sélectionnez l'AMI à utiliser, puis choisissez Select.
4. Suivez l'Assistant pour compléter les pages Choisir un type d'instance et Configurer les détails de l'instance.
5. Sur la page Add Storage, vous pouvez modifier le volume racine, les volumes EBS et les volumes de stockage d'instance de la façon suivante :
 - Pour modifier la taille du volume racine, recherchez le volume Root dans la colonne Type, et modifiez le champ Size.
 - Pour supprimer un volume EBS spécifié par le mappage de périphérique de stockage en mode bloc de l'AMI utilisée pour lancer l'instance, recherchez le volume et cliquez sur l'icône Delete qui lui correspond.
 - Pour ajouter un volume EBS, choisissez Add New Volume (Ajouter un nouveau volume), puis choisissez EBS dans la liste Type et renseignez les champs (Device (Périphérique), Snapshot (Instantané), etc.).
 - Pour supprimer un volume de stockage d'instance spécifié par le mappage de périphérique de stockage en mode bloc de l'AMI utilisée pour lancer l'instance, recherchez le volume et choisissez l'icône Delete qui lui correspond.
 - Pour ajouter un volume de stockage d'instance, choisissez Add New Volume, sélectionnez Instance Store dans la liste Type, puis choisissez un nom de périphérique dans la liste Device.
6. Complétez les pages restantes de l'Assistant, puis sélectionnez Launch.

Command line

Pour ajouter des volumes à une instance à l'aide du AWS CLI

Utilisez la AWS CLI commande [run-instances](#) avec l'option `--block-device-mapping` permettant de spécifier un mappage de périphériques en mode bloc pour une instance au lancement.

Supposons, par exemple, qu'une AMI basée sur EBS spécifie le mappage de périphériques en mode bloc suivant pour une instance Linux :

- `/dev/sdb = ephemeral0`
- `/dev/sdh = snap-1234567890abcdef0`
- `/dev/sdj = 100`

Pour empêcher l'attachement de `/dev/sdj` à une instance lancée à partir de cette AMI, utilisez le mappage suivant.

```
{
  "DeviceName": "/dev/sdj",
  "NoDevice": ""
}
```

Pour augmenter la taille de `/dev/sdh` à 300 GiB, spécifiez le mappage suivant. Notez que vous ne devez pas spécifier l'ID d'instantané pour `/dev/sdh`, car le fait de spécifier le nom du périphérique suffit à identifier le volume.

```
{
  "DeviceName": "/dev/sdh",
  "Ebs": {
    "VolumeSize": 300
  }
}
```

Pour augmenter la taille du volume racine au lancement de l'instance, appelez d'abord [describe-images](#) avec l'ID de l'AMI pour vérifier le nom de l'appareil du volume racine. Par exemple, `"RootDeviceName": "/dev/xvda"`. Pour remplacer la taille du volume racine, spécifiez le nom de l'appareil racine utilisé par l'AMI et la nouvelle taille du volume.

```
{
  "DeviceName": "/dev/xvda",
  "Ebs": {
```

```
    "VolumeSize": 100
  }
}
```

Pour attacher un volume de stockage d'instance supplémentaire, `/dev/sdc`, spécifiez le mappage suivant. Si le type d'instance ne prend pas en charge plusieurs volumes de stockage d'instance, ce mappage n'a aucun effet. Si l'instance prend en charge les volumes de stockage d'instance NVMe, ils sont automatiquement énumérés et un nom d'appareil NVMe leur est attribué.

```
{
  "DeviceName": "/dev/sdc",
  "VirtualName": "ephemeral1"
}
```

Pour ajouter des volumes à une instance à l'aide du AWS Tools for Windows PowerShell

Utilisez le `-BlockDeviceMapping` paramètre avec la [New-EC2Instance](#) commande (AWS Tools for Windows PowerShell).

Mettre à jour le mappage de périphérique de stockage en mode bloc d'une instance en cours d'exécution

Vous pouvez utiliser la AWS CLI commande [modify-instance-attribute](#) pour mettre à jour le mappage des périphériques en mode bloc d'une instance en cours d'exécution. Vous n'avez pas besoin d'arrêter l'instance avant de modifier cet attribut.

```
aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings
file://mapping.json
```

Par exemple, pour conserver le volume racine à la clôture de l'instance, spécifiez les informations suivantes dans le fichier `mapping.json`.

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

```
}  
]
```

Vous pouvez également utiliser le `-BlockDeviceMapping` paramètre avec la [Edit-EC2InstanceAttribute](#) commande (AWS Tools for Windows PowerShell).

Afficher les volumes EBS dans le mappage de périphérique de stockage en mode bloc d'une instance

Vous pouvez facilement énumérer les volumes EBS mappés à une instance.

Note

Pour les instances lancées avant la sortie de l'API 2009-10-31, impossible d'afficher le AWS mappage des périphériques en mode bloc. Vous devez détacher et rattacher les volumes afin de AWS pouvoir afficher le mappage des périphériques en mode bloc.

Console

Pour afficher les volumes EBS pour une instance à l'aide de la console

1. Ouvrez la console Amazon EC2.
2. Dans le panneau de navigation, choisissez Instances.
3. Dans la barre de recherche, saisissez Root device type (Type de périphérique racine), puis sélectionnez EBS. Une liste des instances basées sur des volumes EBS s'affiche.
4. Sélectionnez l'instance souhaitée, puis consultez les informations affichées dans l'onglet Storage (Stockage). Au minimum, les informations suivantes sont disponibles pour le périphérique racine :
 - Root device type (Type de périphérique racine) (par exemple, EBS)
 - Root device name (Nom du périphérique racine) (par exemple, `/dev/xvda`)
 - Block devices (Périphériques de stockage en mode bloc) (par exemple, `/dev/xvda`, `/dev/sdf` et `/dev/sdj`)

Si l'instance a été lancée avec des volumes EBS supplémentaires à l'aide d'un mappage de périphérique de stockage en mode bloc, ceux-ci apparaissent sous Block devices

(Périphériques de stockage en mode bloc). Aucun volume de stockage d'instance n'apparaît sur cet onglet.

5. Pour afficher des informations supplémentaires sur un volume EBS, sélectionnez son ID de volume pour accéder à la page de volume.

Command line

Pour afficher les volumes EBS d'une instance à l'aide de la ligne de commande

Utilisez la commande [describe-instances](#) (AWS CLI) ou la commande [Get-EC2Instance](#) (AWS Tools for Windows PowerShell) pour énumérer les volumes EBS dans le mappage des périphériques en mode bloc pour une instance.

Afficher le mappage de périphérique de stockage en mode bloc d'une instance pour les volumes de stockage d'instances

Le type d'instance détermine le nombre et le type de volumes de stockage d'instance disponibles pour l'instance. Si le nombre de volumes de stockage d'instances dans un mappage d'appareils en bloc dépasse le nombre de volumes de stockage d'instances disponibles pour une instance, les volumes supplémentaires sont ignorés. Pour afficher les volumes de stockage de votre instance, exécutez la `lsblk` commande (instances Linux) ou ouvrez Windows Disk Management (instances Windows). Pour savoir combien de volumes de stockage d'instance sont pris en charge par chaque type d'instance, consultez les spécifications [relatives aux types d'instances Amazon EC2](#).

Lorsque vous affichez le mappage de périphérique de stockage en mode bloc de votre instance, vous pouvez uniquement voir les volumes EBS, mais vous ne pouvez pas voir les volumes de stockage d'instance. La méthode que vous utilisez pour afficher les volumes de stockage d'instance disponibles pour votre instance dépend du type de volume.

Volumes de stockage d'instance NVMe

Instances Linux

Vous pouvez utiliser le package de ligne de commande NVMe, [nvme-cli](#), pour interroger les volumes de stockage d'instance NVMe dans le mappage de périphérique de stockage en mode bloc. Téléchargez et installez le package sur votre instance, puis exécutez la commande suivante.

```
[ec2-user ~]$ sudo nvme list
```

L'exemple ci-dessous présente la sortie pour une instance. Le texte dans la colonne Model indique si le volume est un volume EBS ou un volume de stockage d'instance. Dans cet exemple, /dev/nvme1n1 et /dev/nvme2n1 sont des volumes de stockage d'instance.

Node Namespace	SN	Model	
/dev/nvme0n1	vol06afc3f8715b7a597	Amazon Elastic Block Store	1
/dev/nvme1n1	AWS2C1436F5159EB6614	Amazon EC2 NVMe Instance Storage	1
/dev/nvme2n1	AWSB1F4FF0C0A6C281EA	Amazon EC2 NVMe Instance Storage	1
...			

instances Windows

Vous pouvez utiliser la gestion des disques ou PowerShell répertorier à la fois les volumes EBS et les volumes NVMe de stockage d'instance. Pour plus d'informations, consultez [the section called "Référencer les volumes NVMe"](#).

Volumes de stockage d'instance HDD ou SSD

Vous pouvez utiliser des métadonnées d'instance pour interroger les volumes de stockage d'instances HDD et SSD dans le mappage de périphérique de stockage en mode bloc. Les volumes de stockage d'instances NVMe ne sont pas inclus.

L'URI de base pour toutes les requêtes de métadonnées des instances est <http://169.254.169.254/latest/>. Pour plus d'informations, consultez [Utiliser des métadonnées d'instance](#).

Instances Linux

Commencez par vous connecter à votre instance en cours d'exécution. Utilisez cette requête à partir de l'instance pour obtenir son mappage de périphérique de stockage en mode bloc.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

La réponse inclut les noms des périphériques de stockage en mode bloc de l'instance. Par exemple, la sortie pour une instance `m1.small` basée sur un stockage d'instances ressemble à cela :

```
ami
ephemeral0
root
swap
```

Le périphérique `ami` est le périphérique racine tel que le voit l'instance. Les volumes de stockage d'instance sont nommés `ephemeral[0-23]`. Le périphérique `swap` est utilisé pour le fichier d'échange. Si vous avez également mappé des volumes EBS, ils apparaissent en tant que `ebs1`, `ebs2`, etc.

Pour obtenir des détails relatifs à un périphérique de stockage en mode bloc individuel dans le mappage de périphérique de stockage en mode bloc, ajoutez son nom à la requête précédente, comme illustré ici.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" ` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

instances Windows

Commencez par vous connecter à votre instance en cours d'exécution. Utilisez cette requête à partir de l'instance pour obtenir son mappage de périphérique de stockage en mode bloc.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/
```

La réponse inclut les noms des périphériques de stockage en mode bloc de l'instance. Par exemple, la sortie pour une instance `m1.small` basée sur un stockage d'instances ressemble à cela :

```
ami  
ephemeral0  
root  
swap
```

Le périphérique `ami` est le périphérique racine tel que le voit l'instance. Les volumes de stockage d'instance sont nommés `ephemeral[0-23]`. Le périphérique `swap` est utilisé pour le fichier d'échange. Si vous avez également mappé des volumes EBS, ils apparaissent en tant que `ebs1`, `ebs2`, etc.

Pour obtenir des détails relatifs à un périphérique de stockage en mode bloc individuel dans le mappage de périphérique de stockage en mode bloc, ajoutez son nom à la requête précédente, comme illustré ici.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Mapper des disques sur des volumes sur votre instance Windows

Note

Cette rubrique s'applique uniquement aux instances Windows.

Votre instance Windows est fournie avec un volume EBS qui sert de volume racine. Si votre instance Windows utilise des pilotes AWS PV ou Citrix PV, vous pouvez éventuellement ajouter jusqu'à 25 volumes, soit un total de 26 volumes. Pour plus d'informations, consultez [Limites de volume d'instance](#).

En fonction du type de votre instance, vous disposerez de 0 à 24 volumes de stockage d'instance possibles disponibles pour l'instance. Pour utiliser l'un des volumes de stockage d'instance

disponibles pour votre instance, vous devez spécifier ceux-ci lors de la création de votre AMI ou du lancement de votre instance. Vous pouvez également ajouter des volumes EBS lors de la création de votre AMI ou du lancement de votre instance, ou les attacher pendant l'exécution de celle-ci.

Lorsque vous ajoutez un volume à votre instance, vous spécifiez le nom de l'appareil utilisé par Amazon EC2. Pour de plus amples informations, veuillez consulter [Noms des appareils sur les instances Amazon EC2](#). AWS Les Amazon Machine Images (AMI) Windows contiennent un ensemble de pilotes utilisés par Amazon EC2 pour mapper les volumes de stockage d'instances et EBS aux disques et aux lettres de lecteurs Windows. Si vous lancez une instance à partir d'une AMI Windows qui utilise des pilotes AWS PV ou Citrix PV, vous pouvez utiliser les relations décrites sur cette page pour mapper vos disques Windows à votre magasin d'instances et à vos volumes EBS. Si votre AMI Windows utilise des pilotes PV RedHat, vous pouvez mettre à jour votre instance pour utiliser les pilotes Citrix. Pour plus d'informations, consultez [the section called "Mettre à niveau les pilotes PV"](#).

Table des matières

- [Référencer les volumes NVMe](#)
 - [Référencer les disques NVMe à l'aide de la gestion des disques](#)
 - [Répertoriez les disques NVMe en utilisant PowerShell](#)
 - [Mapper les volumes EBS NVMe](#)
- [Référencer les volumes](#)
 - [Référencer les disques à l'aide de la gestion des disques](#)
 - [Mapper des périphériques de disque aux noms de périphériques](#)
 - [Volumes de stockage d'instance](#)
 - [Volumes EBS](#)
 - [Lister les disques à l'aide PowerShell](#)

Référencer les volumes NVMe

Vous pouvez utiliser la gestion de disques ou Powershell pour rechercher les disques sur votre instance Windows.

Référencer les disques NVMe à l'aide de la gestion des disques

Vous pouvez utiliser la gestion de disques Windows pour rechercher les disques sur votre instance Windows.

Pour rechercher les disques sur votre instance Windows

1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez [Connexion à votre instance Windows](#).
2. Démarrez l'utilitaire Gestion des disques.
3. Examinez les disques. Le volume racine est un volume EBS monté comme C:\. Si aucun autre disque n'est affiché, vous n'avez pas spécifié de volume additionnel lors de la création de l'AMI ou du lancement de l'instance.

L'exemple suivant illustre les disques disponibles si vous lancez une instance r5d.4xlarge avec deux volumes EBS supplémentaires.

Disk Management [Window Title Bar: -, □, X]

File Action View Help

[Navigation icons: back, forward, refresh, help, search, save, print]

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (S...	30.00 GB	13.22 GB	44 %
New Volume (D:)	Simple	Basic	NTFS	Healthy (P...	8.00 GB	7.97 GB	100 %
New Volume (E:)	Simple	Basic	NTFS	Healthy (P...	8.00 GB	7.97 GB	100 %
New Volume (F:)	Simple	Basic	NTFS	Healthy (P...	279.39 GB	279.28 GB	100 %
New Volume (G:)	Simple	Basic	NTFS	Healthy (P...	279.39 GB	279.28 GB	100 %

Disk 0 Basic 30.00 GB Online	(C:) 30.00 GB NTFS Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)
Disk 1 Basic 8.00 GB Online	New Volume (D:) 8.00 GB NTFS Healthy (Primary Partition)
Disk 2 Basic 8.00 GB Online	New Volume (E:) 8.00 GB NTFS Healthy (Primary Partition)
Disk 3 Basic 279.40 GB Online	New Volume (F:) 279.39 GB NTFS Healthy (Primary Partition)
Disk 4 Basic 279.40 GB Online	New Volume (G:) 279.39 GB NTFS Healthy (Primary Partition)

Unallocated
 Primary partition

Répertoriez les disques NVMe en utilisant PowerShell

Le PowerShell script suivant répertorie chaque disque ainsi que le nom de périphérique et le volume correspondants. Il est destiné à être utilisé avec des [instances basées sur le système AWS Nitro](#), qui utilisent NVMe EBS et des volumes de stockage d'instance.

Connectez-vous à votre instance Windows et exécutez la commande suivante pour activer l'exécution du PowerShell script.

```
Set-ExecutionPolicy RemoteSigned
```

Copiez le script suivant et enregistrez-le en tant que `mapping.ps1` sur votre instance Windows.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
    else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
}
```

```
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber = (Get-Disk -Path $Path).Number
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber
}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
        Disk          = $Disk
        Partitions    = $Partition
        DriveLetter   = $DriveLetter
        EbsVolumeId   = $EbsVolumeId
        Device        = $Device
        VirtualDevice = $VirtualDevice
        VolumeName    = $VolumeName
    }
}
```

```
$Report += $Disk
}
```

```
$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Exécutez le script comme suit :

```
PS C:\> .\mapping.ps1
```

Voici un exemple de sortie pour une instance avec un volume racine, deux volumes EBS et deux volumes de stockage d'instance.

Disk	Partitions	DriveLetter	EbsVolumeId	Device	VirtualDevice	VolumeName
0	1	C	vol-03683f1d861744bc7	/dev/sda1	root	
1	1	D	vol-082b07051043174b9	xvdb	N/A	
2	1	E	vol-0a4064b39e5f534a2	xvdc	N/A	
3	1	F	AWS-6AAD8C2AEEE1193F0	Ephemeral	N/A	Temporary
Storage						
4	1	G	AWS-13E7299C2BD031A28	Ephemeral	N/A	Temporary
Storage						

Si vous n'avez pas configuré vos informations d'identification pour Tools for Windows PowerShell sur l'instance Windows, le script ne peut pas obtenir l'ID du volume EBS et utilise N/A dans la EbsVolumeId colonne.

Mapper les volumes EBS NVMe

Avec [les instances basées sur le système AWS Nitro](#), les volumes EBS sont exposés en tant que périphériques NVMe. Vous pouvez utiliser la commande [Get-Disk](#) pour mapper des numéros de disques Windows à des ID de volume EBS.

```
PS C:\> Get-Disk
Number Friendly Name Serial Number HealthStatus
OperationalStatus Total Size Partition
Style
-----
```

3	NVMe Amazo... AWS6AAD8C2AEFF1193F0_00000001. 279.4 GB MBR	Healthy	Online
4	NVMe Amazo... AWS13E7299C2BD031A28_00000001. 279.4 GB MBR	Healthy	Online
2	NVMe Amazo... vol0a4064b39e5f534a2_00000001. 8 GB MBR	Healthy	Online
0	NVMe Amazo... vol03683f1d861744bc7_00000001. 30 GB MBR	Healthy	Online
1	NVMe Amazo... vol082b07051043174b9_00000001. 8 GB MBR	Healthy	Online

Vous pouvez également exécuter la commande `ebsnvme-id` pour mapper les numéros de disque NVMe aux ID de volume EBS et aux noms de périphériques.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Référencer les volumes

Vous pouvez utiliser la gestion de disques ou Powershell pour rechercher les disques sur votre instance Windows.

Référencer les disques à l'aide de la gestion des disques

Vous pouvez utiliser la gestion de disques Windows pour rechercher les disques sur votre instance Windows.

Pour rechercher les disques sur votre instance Windows

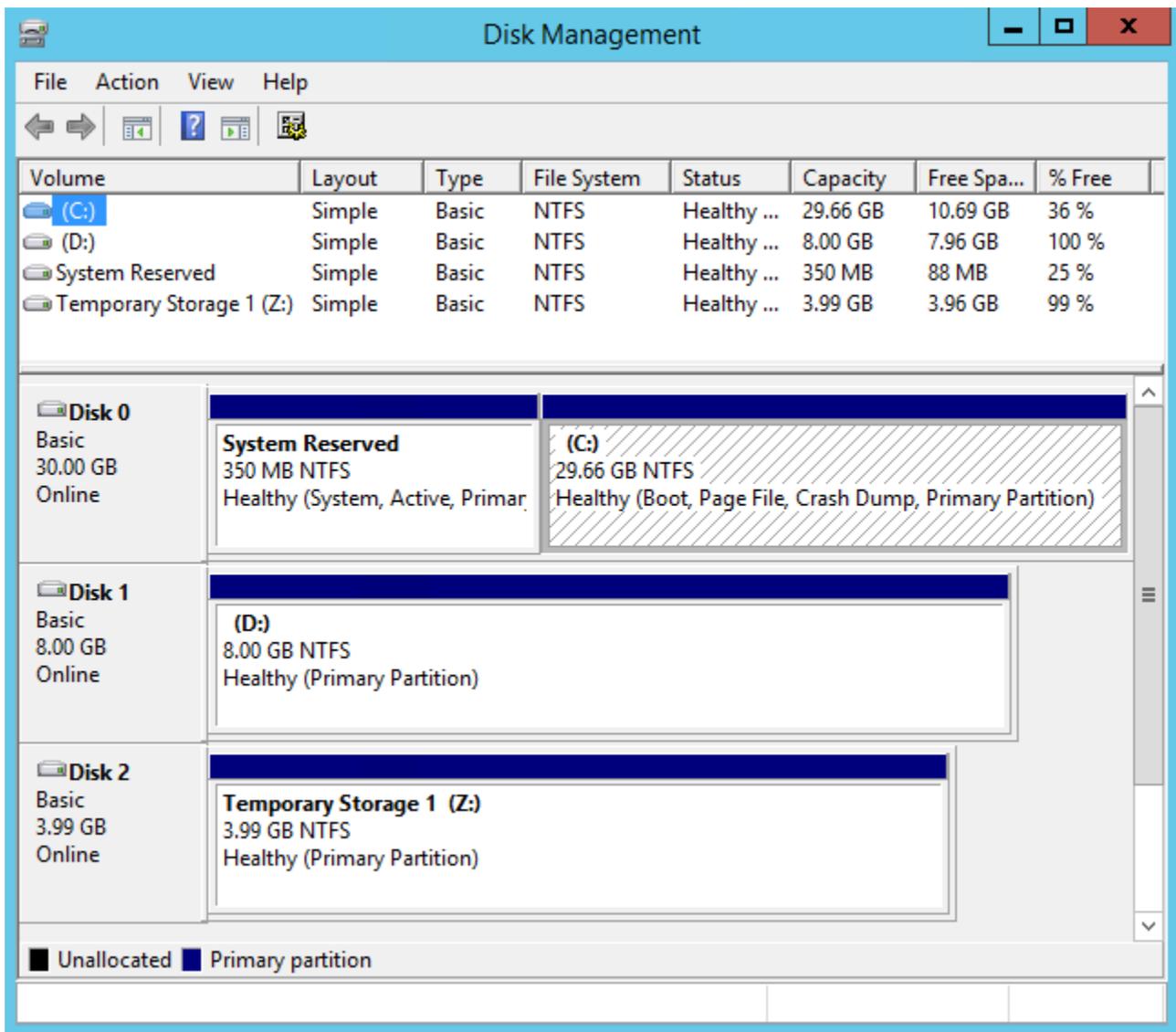
1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez [Connexion à votre instance Windows](#).

2. Démarrez l'utilitaire Gestion des disques.

Dans la barre des tâches, cliquez avec le bouton droit sur le logo Windows, puis sélectionnez Gestion des disques.

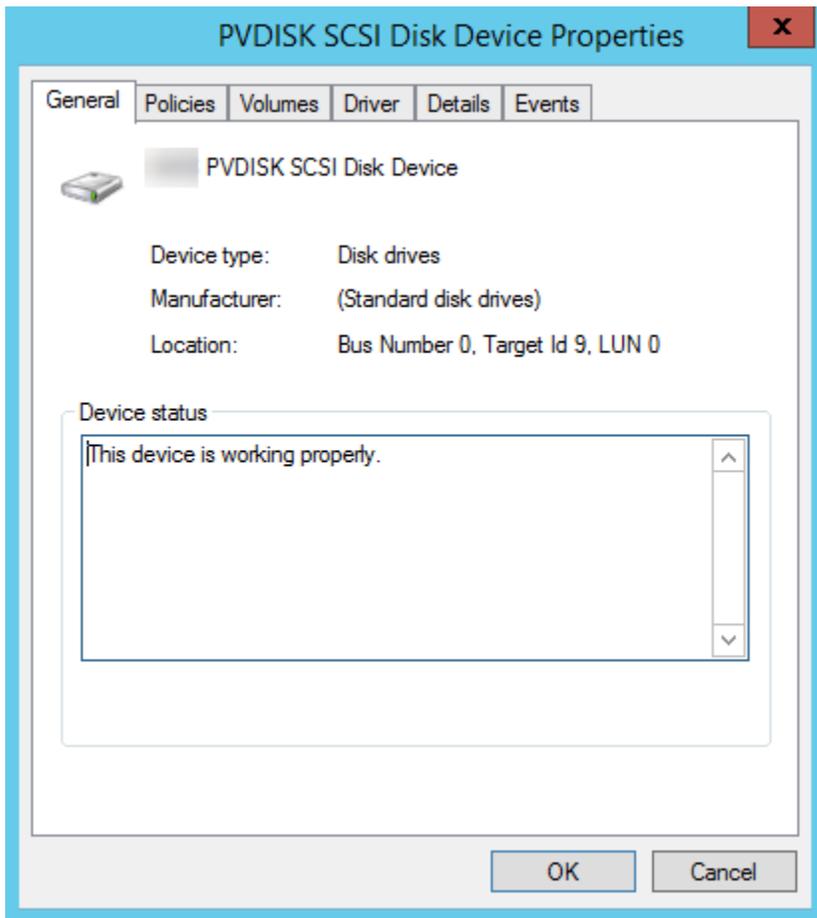
3. Examinez les disques. Le volume racine est un volume EBS monté comme C : \. Si aucun autre disque n'est affiché, vous n'avez pas spécifié de volume additionnel lors de la création de l'AMI ou du lancement de l'instance.

L'exemple suivant affiche les disques qui sont disponibles si vous lancez une instance m3.medium avec un volume basé sur le stockage d'instance (Disk 2) et un volume EBS supplémentaire (Disk 1).



4. Cliquez avec le bouton droit sur le disque 1 étiqueté dans le volet grisé, puis cliquez sur Propriétés. Prenez note de la valeur de l'Emplacement et recherchez-le dans les tables de

[Mapper des périphériques de disque aux noms de périphériques](#). Par exemple, le disque suivant a pour emplacement Bus numéro 0, ID cible 9, LUN 0. D'après la table des volumes EBS, le nom de périphérique de cet emplacement est : xvdj.



Mapper des périphériques de disque aux noms de périphériques

Le pilote du périphérique de stockage en mode bloc de l'instance attribue les noms de volume réels lors du montage des volumes.

Mappages

- [Volumes de stockage d'instance](#)
- [Volumes EBS](#)

Volumes de stockage d'instance

Le tableau suivant décrit comment les pilotes PV et PV Citrix AWS mappent les volumes de stockage d'instances non NVME aux volumes Windows. Le nombre de volumes de stockage d'instance

disponibles est déterminé par le type d'instance. Pour plus d'informations, consultez [Volumes de stockage d'instances](#).

Emplacement	Nom d'appareil
Bus numéro 0, ID cible 78, LUN 0	xvdca
Bus numéro 0, ID cible 79, LUN 0	xvdcb
Bus numéro 0, ID cible 80, LUN 0	xvdcc
Bus numéro 0, ID cible 81, LUN 0	xvdcd
Bus numéro 0, ID cible 82, LUN 0	xvdce
Bus numéro 0, ID cible 83, LUN 0	xvdcf
Bus numéro 0, ID cible 84, LUN 0	xvdcg
Bus numéro 0, ID cible 85, LUN 0	xvdch
Bus numéro 0, ID cible 86, LUN 0	xvdci
Bus numéro 0, ID cible 87, LUN 0	xvdcj
Bus numéro 0, ID cible 88, LUN 0	xvdck
Bus numéro 0, ID cible 89, LUN 0	xvdcl

Volumes EBS

Le tableau suivant décrit comment les pilotes PV et PV Citrix AWS mappent les volumes EBS non NVME aux volumes Windows.

Emplacement	Nom d'appareil
Bus numéro 0, ID cible 0, LUN 0	/dev/sda1
Bus numéro 0, ID cible 1, LUN 0	xvdb

Emplacement	Nom d'appareil
Bus numéro 0, ID cible 2, LUN 0	xvdc
Bus numéro 0, ID cible 3, LUN 0	xvdd
Bus numéro 0, ID cible 4, LUN 0	xvde
Bus numéro 0, ID cible 5, LUN 0	xvdf
Bus numéro 0, ID cible 6, LUN 0	xvdg
Bus numéro 0, ID cible 7, LUN 0	xvdh
Bus numéro 0, ID cible 8, LUN 0	xvdi
Bus numéro 0, ID cible 9, LUN 0	xvdj
Bus numéro 0, ID cible 10, LUN 0	xvdk
Bus numéro 0, ID cible 11, LUN 0	xvdl
Bus numéro 0, ID cible 12, LUN 0	xvdm
Bus numéro 0, ID cible 13, LUN 0	xvdn
Bus numéro 0, ID cible 14, LUN 0	xvdo
Bus numéro 0, ID cible 15, LUN 0	xvdp
Bus numéro 0, ID cible 16, LUN 0	xvdq
Bus numéro 0, ID cible 17, LUN 0	xvdr
Bus numéro 0, ID cible 18, LUN 0	xvds
Bus numéro 0, ID cible 19, LUN 0	xvdt
Bus numéro 0, ID cible 20, LUN 0	xvdu
Bus numéro 0, ID cible 21, LUN 0	xvdv

Emplacement	Nom d'appareil
Bus numéro 0, ID cible 22, LUN 0	xvdw
Bus numéro 0, ID cible 23, LUN 0	xvdx
Bus numéro 0, ID cible 24, LUN 0	xvdy
Bus numéro 0, ID cible 25, LUN 0	xvdz

Lister les disques à l'aide PowerShell

Le PowerShell script suivant répertorie chaque disque ainsi que le nom de périphérique et le volume correspondants.

Exigences et limitations

- Nécessite Windows Server 2012 ou une version ultérieure.
- Nécessite des informations d'identification pour obtenir l'ID de volume EBS. Vous pouvez configurer un profil à l'aide des outils pour PowerShell l'instance ou y associer un rôle IAM.
- Ne prend pas en charge les volumes NVMe.
- Ne prend pas en charge les disques dynamiques.

Connectez-vous à votre instance Windows et exécutez la commande suivante pour activer l'exécution du PowerShell script.

```
Set-ExecutionPolicy RemoteSigned
```

Copiez le script suivant et enregistrez-le en tant que `mapping.ps1` sur votre instance Windows.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
    param([int]$SCSITargetId)
    If ($SCSITargetId -eq 0) {
        return "sda1"
    }
    $deviceName = "xvd"
    If ($SCSITargetId -gt 25) {
        $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
    }
}
```

```
}
$deviceName += [char](0x61 + $SCSITargetId % 26)
return $deviceName
}

[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
    $array1 += $_.Name
    $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
    $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).SerialNumber) -
replace "_[^ ]*$" -replace "vol", "vol-"
    $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).FriendlyName)
    $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
    $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
    $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -ExpandProperty
    SystemName
}
Catch {
    Write-Host "Could not access the instance Metadata using AWS Get-EC2InstanceMetadata
    CMDLet.
    Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and Metadata
    is enabled for this instance." -ForegroundColor Yellow
}
Try {
    $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
    $InstanceId).Instances.BlockDeviceMappings
    $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
    "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
    Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
```

```
Verify that you provided your access keys or assigned an IAM role with adequate
permissions." -ForegroundColor Yellow
}
```

```
Get-disk | ForEach-Object {
    $DriveLetter = $null
    $VolumeName = $null
    $VirtualDevice = $null
    $DeviceName = $_.FriendlyName

    $DiskDrive = $_
    $Disk = $_.Number
    $Partitions = $_.NumberOfPartitions
    $EbsVolumeID = $_.SerialNumber -replace "[^ ]*$" -replace "vol", "vol-"
    if ($Partitions -ge 1) {
        $PartitionsData = Get-Partition -DiskId $_.Path
        $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
    $null) }
        $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
    @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
    }
    If ($DiskDrive.path -like "*PROD_PVDISK*") {
        $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
    Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
    $DiskDrive.Number) }).SCSITargetId)
        $BlockDeviceName = "/dev/" + $BlockDeviceName
        $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*" +
    $_.DeviceName + "*" }
        $EbsVolumeID = $BlockDevice.Ebs.VolumeId
        $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
    $BlockDeviceName }).Key | Select-Object -First 1
    }
    ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
        $BlockDeviceName = (Get-EC2InstanceMetadata -Category
    "BlockDeviceMapping").ephemeral((Get-WmiObject -Class Win32_Diskdrive | Where-Object
    { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)
        $BlockDevice = $null
        $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
    $BlockDeviceName }).Key | Select-Object -First 1
    }
    ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
        if ($DriveLetter -match '^[a-zA-Z0-9]') {
            $i = 0
            While ($i -ne ($array3.Count)) {
```

```

        if ($array[2][$i] -eq $EbsVolumeID) {
            $DriveLetter = $array[0][$i]
            $DeviceName = $array[3][$i]
        }
        $i ++
    }
}
$BlockDevice = ""
$BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.Ebs.VolumeId -eq
$EbsVolumeID }).DeviceName
}
ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '^[a-zA-Z0-9]') {
        $i = 0
        While ($i -ne ($array3.Count)) {
            if ($array[2][$i] -eq $EbsVolumeID) {
                $DriveLetter = $array[0][$i]
                $DeviceName = $array[3][$i]
            }
            $i ++
        }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.Ebs.VolumeId -eq
$EbsVolumeID }).DeviceName
}
Else {
    $BlockDeviceName = $null
    $BlockDevice = $null
}
New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId  = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device       = If ($BlockDeviceName -eq $null) { "N/A" } Else
{ $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName   = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName   = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
}
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions, DriveLetter,
EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName

```

Exécutez le script comme suit :

```
PS C:\> .\mapping.ps1
```

Voici un exemple de sortie.

Disk DeviceName	Partitions	DriveLetter	EbsVolumeId VolumeName	Device	VirtualDevice
0	1	C	vol-0561f1783298efedd	/dev/sda1	N/A
NVMe Amazon Elastic B		N/A			
1	1	D	vol-002a9488504c5e35a	xvdb	N/A
NVMe Amazon Elastic B		N/A			
2	1	E	vol-0de9d46fcc907925d	xvdc	N/A
NVMe Amazon Elastic B		N/A			

Si vous n'avez pas fourni vos informations d'identification sur l'instance Windows, le script ne peut pas obtenir l'ID de volume EBS et indique N/A dans la colonne EbsVolumeId.

Instantanés Amazon EBS basés sur Windows VSS cohérents avec les applications

Note

Les instantanés basés sur Windows VSS cohérents avec les applications ne sont pris en charge qu'avec les instances Windows.

[Vous pouvez prendre des instantanés cohérents avec les applications de tous les volumes Amazon EBS attachés à vos instances Windows Amazon EC2 à l'aide de Run Command.AWS Systems Manager](#) Le processus d'instantané utilise le service [Volume Shadow Copy Service \(VSS\)](#) de Windows pour effectuer des sauvegardes au niveau du volume EBS des applications compatibles avec VSS. Les instantanés incluent des données de transactions en attente entre ces applications et le disque. Vous n'avez pas besoin de fermer vos instances ni de les déconnecter lorsque vous devez sauvegarder tous les volumes attachés.

L'utilisation de snapshots EBS basés sur VSS n'entraîne aucun coût supplémentaire. Vous payez uniquement pour les instantanés EBS créés par le processus de sauvegarde. Pour plus d'informations, consultez [Comment me sont facturés mes instantanés Amazon EBS EBS ?](#)

Table des matières

- [Qu'est-ce qu' VSS ?](#)
- [Prérequis](#)
- [Création d'instantanés EBS compatibles avec VSS](#)
- [Résoudre les problèmes liés aux instantanés EBS basés sur Windows VSS](#)
- [Restaurer des volumes à partir d'instantanés EBS compatibles avec VSS](#)
- [AWS Historique des versions de la solution VSS](#)

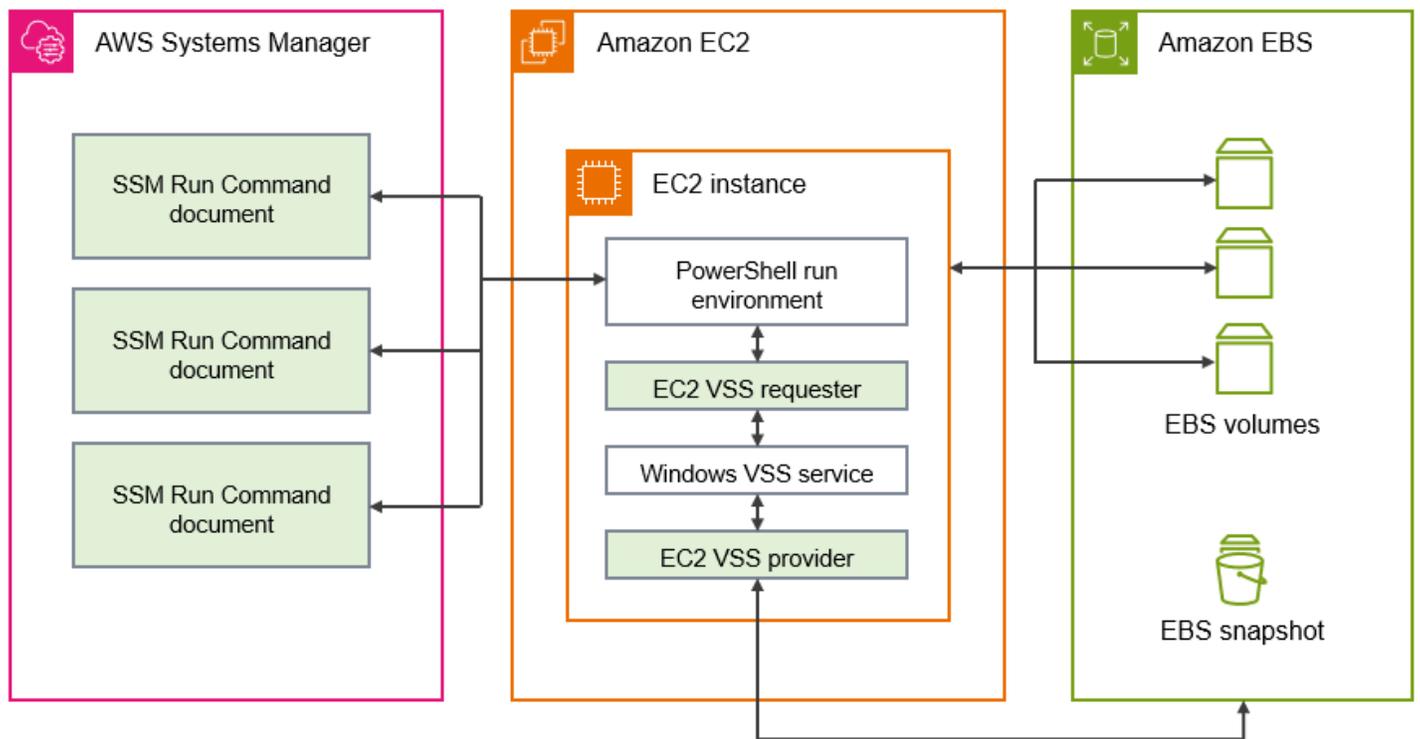
Qu'est-ce qu' VSS ?

Volume Snapshot Copy Service (VSS) est une technologie de sauvegarde et de restauration incluse dans Microsoft Windows. Elle peut créer des copies de sauvegarde, ou des instantanés, de fichiers ou de volumes informatiques pendant leur utilisation. Pour plus d'informations, consultez [Volume Shadow Copy Service](#).

Pour créer un instantané de la cohérence de l'application, les composants logiciels suivants sont impliqués.

- Service VSS : partie intégrante du système d'exploitation Windows
- Demandeur VSS : le logiciel qui demande la création de copies instantanées
- Enregistreur VSS : généralement fourni dans le cadre d'une application, telle que SQL Server, pour garantir un ensemble de données cohérent à sauvegarder
- Fournisseur VSS : le composant qui crée les copies instantanées des volumes sous-jacents

La solution de capture instantanée Amazon EBS basée sur Windows VSS se compose de plusieurs documents Run Command de Systems Manager (SSM) qui facilitent la création de sauvegardes, et d'un [package Systems Manager Distributor](#), appelé `AwsVssComponents`, qui inclut un demandeur EC2 VSS et un fournisseur EC2 VSS. Le package `AwsVssComponents` doit être installé sur les instances Windows EC2 pour prendre des instantanés de volumes EBS de la cohérence de l'application. Le schéma suivant illustre la relation entre ces composants logiciels.



Comment fonctionne la solution de capture instantanée Amazon EBS basée sur VSS

Le processus de création de scripts de capture instantanée EBS basés sur VSS cohérents avec les applications comprend les étapes suivantes.

1. Terminez le [Prérequis](#).
2. Entrez les paramètres du document SSM `AWSEC2-VssInstallAndSnapshot` et exécutez ce document en utilisant Run Command. Pour plus d'informations, consultez [Exécutez le document à AWSEC 2 VssInstallAndSnapshot commandes \(recommandé\)](#).
3. Le service Windows VSS de votre instance coordonne toutes les opérations d'E/S courantes pour les applications en cours d'exécution.
4. Le système vide tous les tampons I/O et suspend provisoirement toutes les opérations d'I/O. Cette interruption dure, au maximum, dix secondes.
5. Pendant cette suspension, le système crée des instantanés de tous les volumes attachés à l'instance.
6. La suspension est ensuite levée et les I/O reprennent leurs opérations.
7. Le système ajoute tous les nouveaux instantanés à la liste des instantanés EBS. Le système étiquette tous les instantanés EBS compatibles VSS créés avec succès par ce processus avec: `true. AppConsistent`

8. Si vous devez effectuer une restauration à partir d'un instantané, vous pouvez utiliser le processus EBS standard de création d'un volume à partir d'un instantané. Vous pouvez également restaurer tous les volumes vers une instance en utilisant un exemple de script. Cette procédure est décrite dans la section [Restaurer des volumes à partir d'instantanés EBS compatibles avec VSS](#).

Prérequis

Vous pouvez créer des instantanés EBS basés sur VSS avec Systems Manager Run Command ou Amazon Data AWS Backup Lifecycle Manager. Les conditions suivantes s'appliquent à toutes les solutions.

Prérequis

- [Configuration système requise](#)
- [Autorisations IAM](#)
- [Composants VSS](#)

Configuration système requise

Installation de l'agent Systems Manager

Le VSS est orchestré par le AWS Systems Manager (Systems Manager) à l'aide de PowerShell. Assurez-vous que vous avez installé SSM Agent version 3.0.502.0 ou une version ultérieure sur votre instance EC2. Si vous utilisez déjà une ancienne version de SSM Agent, mettez-la à jour à l'aide de la fonctionnalité Exécuter la commande. Pour plus d'informations, consultez les sections [Configuration de Systems Manager pour des instances Amazon EC2](#) et [Utilisation de SSM Agent sur des instances Amazon EC2 pour Windows Server](#) dans le Guide de l'utilisateur AWS Systems Manager .

Exigences des instances Windows Amazon EC2

Les instantanés EBS basés sur VSS sont pris en charge pour les instances exécutant Windows Server 2012 et versions ultérieures. Pour les anciennes versions de Windows, consultez le tableau de prise en charge des versions Windows dans [AWS Historique des versions de la solution VSS](#).

Version de .NET Framework

Le package `AwsVssComponents` nécessite .NET Framework version 4.6 ou ultérieure. Les versions du système d'exploitation Windows antérieures à Windows Server 2016 utilisent par

défaut une version antérieure du .NET Framework. Si votre instance utilise une version antérieure du .NET Framework, vous devez installer la version 4.6 ou ultérieure à l'aide de Windows Update.

AWS Tools for Windows PowerShell version

Assurez-vous que votre instance exécute la AWS Tools for Windows PowerShell version 3.3.48.0 ou une version ultérieure. Pour vérifier votre version, exécutez la commande suivante dans le PowerShell terminal de l'instance.

```
C:\> Get-AWSPowerShellVersion
```

Si vous devez effectuer une mise à jour AWS Tools for Windows PowerShell sur votre instance, consultez la section [Installation du AWS Tools for Windows PowerShell](#) dans le guide de AWS Tools for Windows PowerShell l'utilisateur.

PowerShell Version Windows

Assurez-vous que votre instance exécute la version PowerShell majeure de Windows 34, ou 5. Pour vérifier votre version, exécutez la commande suivante dans un PowerShell terminal de l'instance.

```
C:\> $PSVersionTable.PSVersion
```

PowerShell mode linguistique

Assurez-vous que le mode de PowerShell langue de votre instance est défini sur FullLanguage. Pour plus d'informations, veuillez consulter [about_Language_Modes](#) dans la documentation Microsoft.

Autorisations IAM

Le rôle IAM associé à votre instance Windows Amazon EC2 doit être autorisé à créer des instantanés cohérents avec les applications avec VSS. Pour accorder les autorisations nécessaires, vous pouvez associer la `AWSEC2VssSnapshotPolicy` politique à votre profil d'instance.

La politique permet à Systems Manager d'effectuer les actions suivantes :

- Créez et balisez des instantanés EBS

- Création et balisage d'Amazon Machine Images (AMI)
- Attachez des métadonnées, telles que l'ID de l'appareil, aux balises de capture par défaut créées par VSS.

Rubriques

- [Associez la politique de capture instantanée compatible VSS à votre profil d'instance](#)
- [Politique gérée pour créer des instantanés VSS](#)
- [Politique existante \(n'est plus prise en charge\)](#)

Associez la politique de capture instantanée compatible VSS à votre profil d'instance

Pour accorder des autorisations pour les instantanés compatibles VSS pour votre instance, vous devez associer la politique AWSEC2VssSnapshotPolicy gérée à votre rôle de profil d'instance comme suit. Il est important de vous assurer que votre instance répond à toutes les exigences [Configuration système requise](#).

Note

Pour utiliser la politique gérée, la version AwsVssComponents du package 2.3.1 ou une version ultérieure doit être installée sur votre instance. Pour l'historique des versions, voir [AwsVssComponents versions du package](#).

Si une version antérieure du AwsVssComponents package est installée sur votre instance, consultez [Politique en matière d'héritage](#).

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le volet de navigation, choisissez Rôles pour afficher la liste des rôles IAM auxquels vous avez accès.
3. Sélectionnez le lien Nom du rôle associé à votre instance. Cela ouvre la page détaillée du rôle.
4. Pour joindre la politique gérée, choisissez Ajouter des autorisations, dans le coin supérieur droit du panneau de liste. Sélectionnez ensuite Joindre des politiques dans la liste déroulante.
5. Pour rationaliser les résultats, entrez le nom de la politique dans la barre de recherche (AWSEC2VssSnapshotPolicy).
6. Cochez la case à côté du nom de la politique à joindre, puis choisissez Ajouter des autorisations.

Politique gérée pour créer des instantanés VSS

Une politique AWS gérée est une politique autonome proposée par Amazon aux AWS clients. AWS les politiques gérées sont conçues pour accorder des autorisations pour les cas d'utilisation courants. Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Toutefois, vous pouvez copier la politique et l'utiliser comme base de référence pour une [politique gérée par le client](#) spécifique à votre cas d'utilisation.

Pour plus d'informations sur les politiques AWS gérées, voir les [politiques AWS gérées](#) dans le guide de l'utilisateur IAM.

Pour utiliser la `AWSEC2VssSnapshotPolicy` politique, la politique gérée, vous pouvez l'associer au rôle IAM associé à vos instances Windows EC2. Cette politique permet à la solution EC2 VSS de créer et d'ajouter des balises aux Amazon Machine Images (AMI) et aux instantanés EBS. Pour joindre la politique, voir [Associez la politique de capture instantanée compatible VSS à votre profil d'instance](#).

Autorisations octroyées par `AWSEC2VssSnapshotPolicy`

La `AWSEC2VssSnapshotPolicy` politique inclut les autorisations Amazon EC2 suivantes :

- `ec2 : CreateTags` — Ajoutez des balises aux instantanés EBS et aux AMI pour aider à identifier et à classer les ressources.
- `ec2 : DescribeInstance Attribute` — Récupérez les volumes EBS et les mappages de périphériques de blocs correspondants qui sont attachés à l'instance cible.
- `ec2 : CreateSnapshots` — Créez des instantanés des volumes EBS.
- `ec2 : CreateImage` — Créez une AMI à partir d'une instance EC2 en cours d'exécution.
- `ec2 : DescribeImages` — Récupère les informations relatives aux AMI et aux instantanés EC2.
- `ec2 : DescribeSnapshots` — Déterminez l'heure de création et le statut des instantanés afin de vérifier la cohérence de l'application.

Exemple de politique

Voici un exemple de cette `AWSEC2VssSnapshotPolicy` politique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "DescribeInstanceInfo",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeInstanceAttribute"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
        "StringLike": {
            "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
        }
    }
},
{
    "Sid": "CreateSnapshotsWithTag",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateSnapshots"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:snapshot/*"
    ],
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AwsVssConfig": "*"
        }
    }
},
{
    "Sid": "CreateSnapshotsAccessInstance",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateSnapshots"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
        "StringLike": {
            "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
        }
    }
}
},

```

```

    {
      "Sid": "CreateSnapshotsAccessVolume",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshots"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid": "CreateImageWithTag",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateImage"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AwsVssConfig": "*"
        }
      }
    },
    {
      "Sid": "CreateImageAccessInstance",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateImage"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid": "CreateTagsOnResourceCreation",
      "Effect": "Allow",

```

```

    "Action": "ec2:CreateTags",
    "Resource": [
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:image/*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": [
          "CreateImage",
          "CreateSnapshots"
        ]
      }
    }
  },
  {
    "Sid": "CreateTagsAfterResourceCreation",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": [
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:image/*"
    ],
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/AwsVssConfig": "*"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "AppConsistent",
          "Device"
        ]
      }
    }
  },
  {
    "Sid": "DescribeImagesAndSnapshots",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeImages",
      "ec2:DescribeSnapshots"
    ],
    "Resource": "*"
  }
]

```

```
}
```

Simplifier les autorisations pour des cas d'utilisation spécifiques (avancé)

La politique `AWSEC2VssSnapshotPolicy` gérée inclut des autorisations pour toutes les manières dont vous pouvez créer des instantanés compatibles VSS. Vous pouvez créer une politique personnalisée qui inclut uniquement les autorisations dont vous avez besoin.

Cas d'utilisation : créer une AMI, Cas d'utilisation : utiliser AWS Backup un service

Si vous utilisez exclusivement `CreateAmi` cette option ou si vous créez des instantanés compatibles VSS uniquement via le AWS Backup service, vous pouvez rationaliser les déclarations de politique comme suit.

- Omettez les déclarations de politique identifiées par les ID d'instructions (SID) suivants :
 - `CreateSnapshotsWithTag`
 - `CreateSnapshotsAccessInstance`
 - `CreateSnapshotsAccessVolume`
- Ajustez l'`CreateTagsOnResourceCreation` énoncé comme suit :
 - Supprimer `arn:aws:ec2:*:*:snapshot/*` des ressources.
 - Supprimer `CreateSnapshots` de la `ec2:CreateAction` condition.
- Ajustez l'`CreateTagsAfterResourceCreation` instruction pour la `arn:aws:ec2:*:*:snapshot/*` supprimer des ressources.
- Ajustez l'`DescribeImagesAndSnapshots` instruction à supprimer `ec2:DescribeSnapshots` de l'action de la déclaration.

Cas d'utilisation : Snapshot uniquement

Si vous n'utilisez pas `CreateAmi` cette option, vous pouvez rationaliser les déclarations de politique comme suit.

- Omettez les déclarations de politique identifiées par les ID d'instructions (SID) suivants :
 - `CreateImageAccessInstance`
 - `CreateImageWithTag`
- Ajustez l'`CreateTagsOnResourceCreation` énoncé comme suit :
 - Supprimer `arn:aws:ec2:*:*:image/*` des ressources.

- Supprimer `CreateImage` de la `ec2:CreateAction` condition.
- Ajustez l'`CreateTagsAfterResourceCreationInstruction` pour la `arn:aws:ec2:*:*:image/*` supprimer des ressources.
- Ajustez l'`DescribeImagesAndSnapshotsInstruction` à supprimer `ec2:DescribeImages` de l'action de la déclaration.

Note

Pour garantir que votre politique personnalisée fonctionne comme prévu, nous vous recommandons de consulter et d'intégrer régulièrement des mises à jour à la politique gérée.

Politique existante (n'est plus prise en charge)

L'ancienne politique qui accorde l'autorisation pour les instantanés compatibles VSS inclut les autorisations IAM recommandées avant la publication de la politique gérée.

`AWSEC2VssSnapshotPolicy`

Si vous avez configuré un rôle d'instance avec l'ancienne politique, vous pouvez continuer à l'utiliser. Toutefois, pour garantir que votre politique reste à jour avec les meilleures pratiques IAM les plus récentes et que les déclarations de politique s'appliquent en conséquence, nous vous recommandons de remplacer l'ancienne politique par la politique `AWSEC2VssSnapshotPolicy` gérée.

Exemple de politique

L'exemple de politique suivant utilise `ec2:DescribeInstanceAttribute` ce qui est pris en charge dans les versions 2.2.1 et ultérieures `AwsVssComponents` du package. Si une ancienne version du `AwsVssComponents` package est installée, vous devez la remplacer par l'`ec2:DescribeInstancesaction`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": [
        "arn:aws:ec2:*:*:snapshot/*",
```

```
"arn:aws:ec2:*:*:image/*"  
]  
},  
{  
  "Effect": "Allow",  
  "Action": [  
    "ec2:DescribeInstanceAttribute",  
    "ec2:CreateSnapshot",  
    "ec2:CreateSnapshots",  
    "ec2:CreateImage",  
    "ec2:DescribeImages",  
    "ec2:DescribeSnapshots"  
  ],  
  "Resource": "*"   
}  
]  
}
```

Pour plus d'informations sur les politiques gérées par IAM, voir les [politiques AWS gérées](#) dans le Guide de l'utilisateur d'IAM.

Composants VSS

Pour créer des instantanés cohérents avec les applications sur les systèmes d'exploitation Windows, le package `AwsVssComponents` doit être installé sur l'instance. Le package contient un agent VSS EC2 sur instance qui fonctionne en tant que demandeur VSS et fournisseur VSS EC2 pour les volumes EBS.

Il existe plusieurs façons d'installer le composant sur une instance existante :

- (Recommandé) [Exécutez le document à AWSEC 2 VssInstallAndSnapshot commandes \(recommandé\)](#). Cela s'installe ou se met à jour automatiquement si nécessaire à chaque exécution.
- [Installation manuelle de composants VSS sur une instance.](#)
- [Mise à jour des composants VSS sur vos instances selon un calendrier.](#)

Vous pouvez également créer une AMI avec EC2 Image Builder qui utilise le composant géré `aws-vss-components-windows` pour installer le package `AwsVssComponents` pour l'image. Le composant géré utilise AWS Systems Manager Distributor pour installer le package. Une fois qu'Image Builder a créé l'image, le package VSS est installé sur chaque instance que vous lancez depuis l'AMI associée. Pour plus d'informations sur la création d'une AMI sur laquelle le package

VSS est installé, veuillez consulter la rubrique [Distributeur package managed components for Windows](#) dans le Guide de l'utilisateur EC2 Image Builder.

Table des matières

- [Installation manuelle de composants VSS sur une instance](#)
- [Mise à jour des composants VSS sur vos instances selon un calendrier](#)

Installation manuelle de composants VSS sur une instance

Les composants VSS doivent être installés sur votre instance EC2 Windows avant que vous puissiez créer des instantanés cohérents avec l'application à l'aide de Systems Manager. Si vous n'exécutez pas le document de commande `AWSEC2-VssInstallAndSnapshot` pour installer ou mettre à jour automatiquement le package chaque fois que vous créez des instantanés cohérents avec les applications, vous devez installer le package manuellement.

Vous devez également effectuer l'installation manuellement si vous envisagez d'utiliser l'une des méthodes suivantes pour créer des instantanés cohérents avec les applications à partir de votre instance EC2.

- Créez des instantanés VSS à l'aide de AWS Backup
- Création d'instantanés VSS à l'aide d'Amazon Data Lifecycle Manager

Si vous devez effectuer une installation manuelle, nous vous recommandons d'utiliser le dernier package de composants AWS VSS pour améliorer la fiabilité et les performances des instantanés cohérents avec les applications sur vos instances Windows EC2.

Note

Pour installer ou mettre à jour automatiquement le package `AwsVssComponents` chaque fois que vous créez des instantanés cohérents avec les applications, nous vous recommandons d'utiliser Systems Manager pour exécuter le document `AWSEC2-VssInstallAndSnapshot`. Pour plus d'informations, consultez [Exécutez le document à AWSEC 2 VssInstallAndSnapshot commandes \(recommandé\)](#).

Pour installer les composants VSS sur une instance Windows Amazon EC2, suivez les étapes correspondant à votre environnement préféré.

Console

Pour installer les composants VSS à l'aide de SSM Distributor

1. Ouvrez la AWS Systems Manager console à l'[adresse https://console.aws.amazon.com/systems-manager/](https://console.aws.amazon.com/systems-manager/).
2. Dans le panneau de navigation, choisissez Fonctionnalité Exécuter la commande.
3. Choisissez Run Command (Exécuter la commande).
4. Pour le document de commande, cliquez sur le bouton à côté de AWS-Configure AWSPackage.
5. Dans Command parameters (Paramètres de la commande), procédez comme suit :
 - a. Vérifiez que l'option Action est définie sur Install (Installer).
 - b. Pour Nom, saisissez `AwsVssComponents`.
 - c. Pour Version, saisissez un numéro de version ou laissez le champ vide pour que Systems Manager installe la dernière version.
6. Dans la section Targets (Cibles), identifiez les instances sur lesquelles vous souhaitez exécuter cette opération en spécifiant les balises ou en sélectionnant manuellement les instances.

Note

Si vous choisissez de sélectionner les instances manuellement et qu'une instance que vous vous attendez à voir ne figure pas dans la liste, consultez [Où sont mes instances ?](#) dans le Guide de l'utilisateur AWS Systems Manager pour obtenir des conseils de résolution d'incident.

7. Pour Autres paramètres :
 - (Facultatif) Pour Comment (Commentaire), saisissez les informations relatives à cette commande.
 - Pour Délai (secondes), précisez le nombre de secondes durant lesquelles le système doit attendre avant de mettre en échec l'exécution de la commande globale.
8. (Facultatif) Pour Contrôle du débit :
 - Pour Concurrency (Simultanéité), spécifiez un nombre ou un pourcentage d'instances sur lesquelles exécuter simultanément la commande.

Note

Si vous avez sélectionné des cibles en choisissant des balises Amazon EC2, et que vous n'êtes pas sûr du nombre d'instances qui utilisent les balises sélectionnées, limitez le nombre d'instances pouvant exécuter simultanément le document en spécifiant un pourcentage.

- Pour Seuil d'erreur, spécifiez quand arrêter l'exécution de la commande sur d'autres instances après son échec sur un nombre ou un pourcentage d'instances. Si, par exemple, vous spécifiez trois erreurs, Systems Manager cesse d'envoyer la commande à la réception de la quatrième erreur. Les instances sur lesquelles la commande est en cours de traitement peuvent également envoyer des erreurs.
9. (Facultatif) Dans la section Output options (Options de sortie), si vous souhaitez enregistrer la sortie de la commande dans un fichier, sélectionnez Enable writing to an S3 bucket (Autoriser l'écriture dans un compartiment S3) Spécifiez les noms du compartiment et (facultatif) du préfixe (dossier).

Note

Les autorisations S3 qui accordent la possibilité d'écrire les données dans un compartiment S3 sont celles du profil d'instance attribué à l'instance, et non celles de l'utilisateur qui effectue cette tâche. Pour plus d'informations, consultez [Créer un profil d'instance IAM pour Systems Manager](#) dans le Guide de l'utilisateur AWS Systems Manager .

10. (Facultatif) Spécifiez les options pour les notifications SNS.

Pour plus d'informations sur la configuration des notifications Amazon SNS pour Run Command, consultez [Configuration des notifications Amazon SNS pour AWS Systems Manager](#).

11. Cliquez sur Exécuter.

AWS CLI

Utilisez la procédure suivante pour télécharger et installer le package `AwsVssComponents` sur vos instances en utilisant Run Command depuis AWS CLI. Le programme installe deux

composants : un demandeur VSS et un fournisseur VSS. Le système copie ces composants dans un répertoire sur l'instance, puis enregistre la DLL du fournisseur comme fournisseur VSS.

Pour installer le package VSS à l'aide du AWS CLI

- Exécutez la commande suivante pour télécharger et installer les composants VSS requis pour Systems Manager.

```
aws ssm send-command \  
  --document-name "AWS-ConfigureAWSPackage" \  
  --instance-ids "i-01234567890abcdef" \  
  --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Suivez la procédure ci-dessous pour télécharger et installer le `AwsVssComponents` package sur vos instances à l'aide de la commande Exécuter la commande depuis les outils pour Windows PowerShell. Le programme installe deux composants : un demandeur VSS et un fournisseur VSS. Le système copie ces composants dans un répertoire sur l'instance, puis enregistre la DLL du fournisseur comme fournisseur VSS.

Pour installer le package VSS à l'aide du AWS Tools for Windows PowerShell

- Exécutez la commande suivante pour télécharger et installer les composants VSS requis pour Systems Manager.

```
Send-SSMCommand -DocumentName AWS-ConfigureAWSPackage -InstanceId  
"i-01234567890abcdef" -Parameter  
@{'action'='Install';'name'='AwsVssComponents'}
```

Vérifiez la signature sur les composants AWS VSS

Utilisez la procédure suivante pour vérifier la signature sur le package `AwsVssComponents`.

1. Connectez-vous à votre instance Windows. Pour plus d'informations, consultez [Connexion à votre instance Windows](#).
2. Accédez à `C:\Program Files\Amazon\AwsVss Components`.
3. Ouvrez le menu contextuel (clic droit) pour `ec2-vss-agent.exe`, puis choisissez Propriétés.

4. Accédez à l'onglet Signatures numériques et vérifiez que le nom du signataire est Amazon Web Services Inc.
5. Suivez les étapes précédentes pour vérifier la signature sur `Ec2VssInstaller` et `Ec2VssProvider.dll`.

Mise à jour des composants VSS sur vos instances selon un calendrier

Nous vous recommandons de maintenir les composants VSS à jour avec la dernière version recommandée. Il existe plusieurs façons de mettre à jour les composants lorsqu'une nouvelle version du package `AwsVssComponents` est publiée.

Méthodes de mise à jour

- Vous pouvez répéter les étapes décrites [Installation manuelle de composants VSS sur une instance](#) lors de la publication d'une nouvelle version des composants AWS VSS.
- Vous pouvez configurer une association Systems Manager State Manager pour télécharger et installer automatiquement de nouveaux composants VSS ou des composants mis à jour lorsque le package `AwsVssComponents` est disponible.
- Vous pouvez installer ou mettre à jour automatiquement le package `AwsVssComponents` chaque fois que vous créez des instantanés cohérents avec les applications, lorsque vous utilisez Systems Manager pour exécuter le document `AWSEC2-VssInstallAndSnapshot`.

Note

Nous vous recommandons d'utiliser Systems Manager pour exécuter le document de commande `AWSEC2-VssInstallAndSnapshot`, qui installe ou met à jour automatiquement le package `AwsVssComponents` avant qu'il ne crée les instantanés cohérents avec les applications. Pour plus d'informations, consultez [Exécutez le document à AWSEC 2 VssInstallAndSnapshot commandes \(recommandé\)](#).

Pour créer une association Systems Manager State Manager, suivez les étapes correspondant à votre environnement préféré.

Console

Pour créer une association State Manager à l'aide de la console

1. Ouvrez la AWS Systems Manager console à l'[adresse https://console.aws.amazon.com/systems-manager/](https://console.aws.amazon.com/systems-manager/).

2. Dans le volet de navigation, sélectionnez State Manager.

Ou, si la page d'accueil de Systems Manager s'ouvre en premier, ouvrez le volet de navigation, puis choisissez State Manager.

3. Sélectionnez Créer une association.
4. Dans le champ Name (Nom), saisissez un nom évocateur.
5. Dans la liste des documents, choisissez AWSPackageAWS-Configure.
6. Dans la section Paramètres, sélectionnez Installer dans la liste Action.
7. Pour Installation type (Type d'installation), sélectionnez Uninstall and reinstall (Désinstaller et réinstaller).
8. Dans le champ Nom, saisissez `AwsVssComponents`. Vous pouvez ne rien inscrire dans les champs Version et Additional Arguments (Arguments supplémentaires).
9. Dans la section Targets (Cibles), sélectionnez une option.

Note

Si vous choisissez de cibler les instances à l'aide de balises, et que vous spécifiez des balises qui correspondent à des instances Linux, l'association réussit sur l'instance Windows, mais échoue sur les instances Linux. Le statut global de l'association indique Failed.

10. Dans la section Spécifier le programme, sélectionnez une option.
11. Dans la section Advanced options (Options avancées), pour Compliance severity (Sévérité de conformité), sélectionnez un niveau de sévérité pour l'association. Pour de plus amples informations, consultez [A propos de la conformité des associations State Manager](#). Pour les Calendriers de modifications, sélectionnez un calendrier de modifications préconfiguré. Pour de plus amples informations, consultez [AWS Systems Manager Change Calendar](#).
12. Pour Contrôle du débit, procédez comme suit :


```
--parameters '{"action":["Install"],"installationType":["Uninstall and  
reinstall"],"name":["AwsVssComponents']}' \\  
--targets [{"Key\":"InstanceIds\","\Values\":["i-01234567890abcdef\  
i-000011112222abcde\"]}]
```

Pour plus d'informations sur les autres options que vous pouvez utiliser avec la `create-association` commande, voir [create-association](#) dans la AWS Systems Manager section de la référence des AWS CLI commandes.

Création d'instantanés EBS compatibles avec VSS

Cette section présente les étapes pour la création d'instantanés EBS compatibles avec VSS.

Vous pouvez créer des instantanés EBS compatibles avec VSS de volumes EBS attachés à vos instances EC2. Avant de tenter de créer un instantané compatible avec VSS, assurez-vous que les exigences décrites dans la rubrique [Prérequis](#) sont satisfaites.

Rubriques

- [Création d'instantanés VSS à l'aide des documents de commande AWS Systems Manager](#)
- [Créez des instantanés VSS à l'aide de AWS Backup](#)
- [Création d'instantanés VSS à l'aide d'Amazon Data Lifecycle Manager](#)

Création d'instantanés VSS à l'aide des documents de commande AWS Systems Manager

Vous pouvez utiliser des documents de commande de AWS Systems Manager pour créer des instantanés compatibles VSS. Le contenu suivant présente les documents de commande disponibles et les paramètres d'exécution utilisés par ces documents pour créer vos instantanés.

Avant d'utiliser l'un des documents de commande de Systems Manager, assurez-vous d'avoir respecté toutes les [Prérequis](#).

Rubriques

- [Paramètres des documents d'instantanés VSS Systems Manager](#)
- [Exécution de documents de commande d'instantanés VSS Systems Manager](#)

Paramètres des documents d'instantanés VSS Systems Manager

Les documents Systems Manager qui créent des instantanés VSS utilisent tous les paramètres suivants, sauf indication contraire :

ExcludeBootVolume (chaîne, facultatif)

Ce paramètre exclut les volumes de démarrage du processus de sauvegarde si vous créez des instantanés. Pour exclure les volumes de démarrage de vos instantanés, définissez ExcludeBootVolume sur `True` et CreateAmi sur `False`.

Si vous créez une AMI pour votre sauvegarde, ce paramètre doit être défini sur `False`. La valeur par défaut de ce paramètre est `False`.

NoWriters(chaîne, facultatif)

Définissez ce paramètre sur `True` pour exclure les enregistreurs VSS d'application du processus de capture instantanée. L'exclusion d'enregistreurs VSS d'application peut vous aider à résoudre les conflits avec des composants de sauvegarde VSS tiers. La valeur par défaut de ce paramètre est `False`.

CopyOnly(chaîne, facultatif)

Si vous utilisez la sauvegarde native de SQL Server en plus de AWS VSS, l'exécution d'une sauvegarde avec copie uniquement empêche AWS VSS de rompre la chaîne de sauvegarde différentielle native. Pour effectuer une opération de sauvegarde par copie uniquement, définissez ce paramètre sur `True`.

La valeur par défaut de ce paramètre est `False`, ce qui oblige AWS VSS à effectuer une opération de sauvegarde complète.

CreateAmi(chaîne, facultatif)

Pour créer une Amazon Machine Image (AMI) compatible AVEC VSS afin de sauvegarder votre instance, définissez ce paramètre sur `True`. La valeur par défaut de ce paramètre est `False`, qui sauvegarde votre instance avec un instantané EBS à la place.

Pour plus d'informations sur la création d'une AMI à partir d'une instance , consultez la page [Création d'une AMI basée sur Amazon EBS](#).

AmiName(chaîne, facultatif)

Si l'CreateAmi option est définie sur `True`, spécifiez le nom de l'AMI créée par la sauvegarde.

description : (chaîne, facultatif)

Spécifiez une description pour les instantanés ou les images créés par ce processus.

tags (chaîne, facultatif)

Nous vous recommandons de baliser vos instantanés et vos images pour vous aider à localiser et à gérer vos ressources, par exemple pour restaurer des volumes à partir d'une liste d'instantanés. Le système ajoute la Name clé, avec une valeur vide dans laquelle vous pouvez spécifier le nom que vous souhaitez appliquer à vos instantanés ou images de sortie.

Si vous souhaitez spécifier des balises supplémentaires, séparez-les par un point-virgule entre les deux. Par exemple, `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

Par défaut, le système ajoute les balises réservées suivantes pour les instantanés et les images compatibles VSS.

- **Appareil** : pour les instantanés compatibles VSS, il s'agit du nom de périphérique du volume EBS capturé par le cliché.
- **AppConsistent**— Cette balise indique la création réussie d'un instantané ou d'une AMI compatible VSS.
- **AwsVssConfig** — Cela identifie les instantanés et les AMI créés avec le VSS activé. La balise inclut des méta-informations telles que la `AwsVssComponents` version.

 Warning

La spécification de l'une de ces balises réservées dans votre liste de paramètres provoquera une erreur.

executionTimeout (chaîne, facultatif)

Indiquez la durée maximale en secondes pour exécuter le processus de création d'instantanés sur l'instance ou pour créer une AMI à partir de l'instance. L'augmentation de ce délai d'expiration permet à la commande d'attendre plus longtemps pour que VSS commence à se figer et termine le balisage des ressources qu'elle crée. Ce délai ne s'applique qu'aux étapes de création d'instantané ou d'AMI. L'étape initiale d'installation ou de mise à jour du package `AwsVssComponents` n'est pas incluse dans le délai d'expiration.

CollectDiagnosticLogs (chaîne, facultatif)

Pour collecter plus d'informations lors des étapes de création de snapshots et d'AMI, définissez ce paramètre sur « True ». La valeur par défaut de ce paramètre est « False ». Les journaux de diagnostic consolidés sont enregistrés sous .zip forme d'archive au format à l'emplacement suivant sur votre instance :

```
C:\ProgramData\Amazon\AwsVss\Logs\timestamp.zip
```

VssVersion(chaîne, facultatif)

Pour le document AWSEC2-VssInstallAndSnapshot uniquement, vous pouvez spécifier le paramètre VssVersion pour installer une version spécifique du package AwsVssComponents sur votre instance. Laissez ce paramètre vide pour installer la version par défaut recommandée.

Si la version spécifiée du package AwsVssComponents est déjà installée, le script ignore l'étape d'installation et passe à l'étape de sauvegarde. Pour obtenir la liste des versions de package AwsVssComponents et du support d'exploitation, consultez [AWS Historique des versions de la solution VSS](#).

Exécution de documents de commande d'instantanés VSS Systems Manager

Vous pouvez créer des instantanés EBS compatibles VSS avec des documents de AWS Systems Manager commande comme suit.

Exécutez le document à AWSEC 2 VssInstallAndSnapshot commandes (recommandé)

Lorsque vous exécutez AWS Systems Manager le AWSEC2-VssInstallAndSnapshot document, le script exécute les étapes suivantes.

1. Le script commence par installer ou mettre à jour le package AwsVssComponents sur votre instance, selon qu'il est déjà installé ou non.
2. Le script crée les instantanés cohérents avec l'application une fois la première étape terminée.

Pour exécuter le document AWSEC2-VssInstallAndSnapshot, suivez les étapes correspondant à votre environnement préféré.

Console

Création d'instantanés EBS compatibles avec VSS depuis la console

1. Ouvrez la AWS Systems Manager console à l'[adresse https://console.aws.amazon.com/systems-manager/](https://console.aws.amazon.com/systems-manager/).
2. Dans le volet de navigation, sélectionnez Exécuter une commande. Cela permet d'afficher une liste des commandes en cours d'exécution dans votre compte, le cas échéant.
3. Sélectionnez Run Command (Exécuter la commande). Cela permet d'ouvrir la liste des documents de commande auxquels vous avez accès.
4. Sélectionnez AWSEC2-VssInstallAndSnapshot dans la liste des documents de commande. Pour rationaliser les résultats, vous pouvez saisir tout ou partie du nom du document. Vous pouvez également filtrer par propriétaire, par type de plateforme ou par balise.

Lorsque vous sélectionnez un document de commande, les détails apparaissent sous la liste.

5. Sélectionnez Default version at runtime dans la liste Version du document.
6. Configurez les paramètres de commande pour définir la manière dont AWSEC2-VssInstallAndSnapshot va installer le package AwsVssComponents et va effectuer une sauvegarde à l'aide d'une AMI ou d'instantanés VSS. Pour plus de détails sur les paramètres, veuillez consulter la rubrique [Paramètres des documents d'instantanés VSS Systems Manager](#).
7. Pour Sélection de la cible, spécifiez des balises ou sélectionnez des instances manuellement afin d'identifier les instances sur lesquelles vous souhaitez exécuter cette opération.

Note

Si vous sélectionnez les instances manuellement et qu'une instance que vous vous attendez à voir ne figure pas dans la liste, consultez [Où sont mes instances ?](#) pour obtenir des conseils de résolution d'incident.

8. Pour des paramètres supplémentaires permettant de définir le comportement de Exécuter la commande Systems Manager, tels que Contrôle du débit, entrez des valeurs comme décrit dans [Exécution des commande à partir de la console](#).
9. Cliquez sur Run (Exécuter).

En cas de réussite, la commande complète automatiquement la liste des instantanés EBS avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des instantanés EBS en recherchant les balises que vous avez précisées ou en recherchant `AppConsistent`. Si l'exécution de la commande a échoué, consultez la sortie de commande Systems Manager pour en connaître les raisons. Si la commande a réussi mais que la sauvegarde d'un volume spécifique a échoué, vous pouvez résoudre l'échec dans la liste des volumes EBS.

AWS CLI

Vous pouvez exécuter les commandes suivantes dans le AWS CLI pour créer des instantanés EBS compatibles VSS et obtenir l'état de la création de vos instantanés.

Création d'instantanés EBS compatibles avec VSS

Exécutez la commande suivante pour créer des instantanés EBS activés pour VSS. Pour créer les instantanés, vous devez identifier les instances à l'aide du paramètre `--instance-ids`. Pour plus d'informations sur les autres paramètres que vous pouvez utiliser, veuillez consulter la rubrique [Paramètres des documents d'instantanés VSS Systems Manager](#).

```
aws ssm send-command \  
  --document-name "AWSEC2-VssInstallAndSnapshot" \  
  --instance-ids "i-01234567890abcdef" \  
  --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":  
  ["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

En cas de réussite, le document de commande complète automatiquement la liste des instantanés EBS avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des instantanés EBS en recherchant les balises que vous avez précisées ou en recherchant `AppConsistent`. Si l'exécution de la commande a échoué, consultez la sortie de commande pour en connaître les raisons.

Obtenir le statut de la commande

Pour obtenir l'état actuel des instantanés, exécutez la commande suivante à l'aide de l'ID de commande renvoyé par `send-command`.

```
aws ssm get-command-invocation
```

```
--instance-ids "i-01234567890abcdef" \  
--command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \  
--plugin-name "CreateVssSnapshot"
```

PowerShell

Exécutez les commandes suivantes AWS Tools for Windows PowerShell pour créer des instantanés EBS compatibles VSS et obtenir l'état d'exécution actuel pour la création de votre sortie. Spécifiez les paramètres décrits dans la liste précédente pour modifier le comportement du processus de capture instantanée.

Créez des instantanés EBS compatibles VSS avec Tools for Windows PowerShell

Exécutez la commande suivante pour créer des AMI ou des instantanés EBS compatible avec VSS.

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId  
"i-01234567890abcdef" -Parameter  
{'ExcludeBootVolume'='False';'description'='a_description'  
;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Obtenir le statut de la commande

Pour obtenir l'état actuel des instantanés, exécutez la commande suivante à l'aide de l'ID de commande renvoyé par Send-SSMCommand.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId  
"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

En cas de réussite, la commande complète automatiquement la liste des instantanés EBS avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des instantanés EBS en recherchant les balises que vous avez précisées ou en recherchant AppConsistent. Si l'exécution de la commande a échoué, consultez la sortie de commande pour en connaître les raisons.

Exécutez le document de CreateVssSnapshot commande à AWSEC 2

Pour exécuter le document AWSEC2-CreateVssSnapshot, suivez les étapes correspondant à votre environnement préféré.

Console

Création d'instantanés EBS compatibles avec VSS depuis la console

1. Ouvrez la AWS Systems Manager console à l'[adresse https://console.aws.amazon.com/systems-manager/](https://console.aws.amazon.com/systems-manager/).
2. Dans le volet de navigation, sélectionnez Exécuter une commande. Cela permet d'afficher une liste des commandes en cours d'exécution dans votre compte, le cas échéant.
3. Sélectionnez Run Command (Exécuter la commande). Cela permet d'ouvrir la liste des documents de commande auxquels vous avez accès.
4. Sélectionnez AWSEC2-CreateVssSnapshot dans la liste des documents de commande. Pour rationaliser les résultats, vous pouvez saisir tout ou partie du nom du document. Vous pouvez également filtrer par propriétaire, par type de plateforme ou par balise.

Lorsque vous sélectionnez un document de commande, les détails apparaissent sous la liste.

5. Sélectionnez `Default version at runtime` dans la liste Version du document.
6. Configurez les Paramètres de la commande pour définir la manière dont AWSEC2-CreateVssSnapshot effectuera la sauvegarde avec des instantanés VSS ou une AMI. Pour plus de détails sur les paramètres, veuillez consulter la rubrique [Paramètres des documents d'instantanés VSS Systems Manager](#).
7. Pour Sélection de la cible, spécifiez des balises ou sélectionnez des instances manuellement afin d'identifier les instances sur lesquelles vous souhaitez exécuter cette opération.

Note

Si vous sélectionnez les instances manuellement et qu'une instance que vous vous attendez à voir ne figure pas dans la liste, consultez [Où sont mes instances ?](#) pour obtenir des conseils de résolution d'incident.

8. Pour des paramètres supplémentaires permettant de définir le comportement de Exécuter la commande Systems Manager, tels que Contrôle du débit, entrez des valeurs comme décrit dans [Exécution des commande à partir de la console](#).
9. Cliquez sur Run (Exécuter).

En cas de réussite, la commande complète automatiquement la liste des instantanés EBS avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des instantanés EBS en recherchant les balises que vous avez précisées ou en recherchant

AppConsistent. Si l'exécution de la commande a échoué, consultez la sortie de commande Systems Manager pour en connaître les raisons. Si la commande a réussi mais que la sauvegarde d'un volume spécifique a échoué, vous pouvez résoudre l'échec dans la liste des volumes EBS.

AWS CLI

Vous pouvez exécuter la commande suivante dans le AWS CLI pour créer des instantanés EBS compatibles VSS.

Création d'instantanés EBS compatibles avec VSS

Exécutez la commande suivante pour créer des instantanés EBS activés pour VSS. Pour créer les instantanés, vous devez identifier les instances à l'aide du paramètre `--instance-ids`. Pour plus d'informations sur les autres paramètres que vous pouvez utiliser, veuillez consulter la rubrique [Paramètres des documents d'instantanés VSS Systems Manager](#).

```
aws ssm send-command \  
  --document-name "AWSEC2-CreateVssSnapshot" \  
  --instance-ids "i-01234567890abcdef" \  
  --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":  
  [{"Key=key_name,Value=tag_value}]}'
```

En cas de réussite, le document de commande complète automatiquement la liste des instantanés EBS avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des instantanés EBS en recherchant les balises que vous avez précisées ou en recherchant AppConsistent. Si l'exécution de la commande a échoué, consultez la sortie de commande pour en connaître les raisons.

PowerShell

Exécutez la commande suivante AWS Tools for Windows PowerShell pour créer des instantanés EBS compatibles VSS.

Créer des instantanés EBS compatibles VSS avec Tools for Windows PowerShell

Exécutez la commande suivante pour créer des instantanés EBS activés pour VSS. Pour créer les instantanés, vous devez identifier les instances à l'aide du paramètre `InstanceId`. Vous pouvez spécifier plusieurs instances pour lesquelles créer des instantanés. Pour plus d'informations sur

les autres paramètres que vous pouvez utiliser, veuillez consulter la rubrique [Paramètres des documents d'instantanés VSS Systems Manager](#).

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
"i-01234567890abcdef" -Parameter
@{'ExcludeBootVolume'='False';'description'='a_description'
;'tags'='Key=key_name,Value=tag_value'}
```

En cas de réussite, la commande complète automatiquement la liste des instantanés EBS avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des instantanés EBS en recherchant les balises que vous avez précisées ou en recherchant AppConsistent. Si l'exécution de la commande a échoué, consultez la sortie de commande pour en connaître les raisons. Si la commande a réussi mais que la sauvegarde d'un volume spécifique a échoué, vous pouvez résoudre l'échec dans la liste des instantanés EBS.

Exécution de documents de commande pour un cluster de basculement Windows avec stockage EBS partagé

Vous pouvez utiliser l'une des procédures de ligne de commande décrites dans la section précédente pour créer un instantané compatible avec VSS. Le document de commande (AWSEC2-VssInstallAndSnapshot ou AWSEC2-CreateVssSnapshot) doit être exécuté sur le nœud primaire de votre cluster. Le document échoue sur les nœuds secondaires, car ils n'ont pas accès aux disques partagés. Si vos paramètres principal et secondaire changent de manière dynamique, vous pouvez exécuter le document AWS Systems Manager Exécuter la commande sur plusieurs nœuds en espérant que la commande réussira sur le nœud principal et échouera sur les nœuds secondaires.

Exécutez le AWSEC document de commande ManageVss 2-IO SSM

Vous pouvez utiliser le script suivant et le document SSM AWSEC2-ManageVssIO prédéfini pour suspendre provisoirement les I/O, créer des instantanés EBS activés pour VSS, puis redémarrer les I/O. Si l'utilisateur dispose des autorisations suffisantes pour créer et étiqueter des instantanés, il AWS Systems Manager peut créer et étiqueter des instantanés EBS compatibles VSS sans avoir besoin du rôle de snapshot IAM supplémentaire sur l'instance.

Par contre, le document de commande (AWSEC2-VssInstallAndSnapshot ou AWSEC2-CreateVssSnapshot) requiert l'attribution du rôle d'instantané IAM à chaque instance pour laquelle vous souhaitez créer des instantanés EBS. Si, pour des raisons de politique ou de conformité, vous

ne souhaitez pas fournir d'autorisations IAM supplémentaires pour vos instances, vous pouvez utiliser le script suivant.

Avant de commencer

Notez les informations importantes suivantes sur ce processus :

- Ce processus utilise un PowerShell script (`CreateVssSnapshotAdvancedScript.ps1`) pour prendre des instantanés de tous les volumes sur les instances que vous spécifiez, à l'exception des volumes racine. Si vous avez besoin de prendre des instantanés des volumes racines, vous devez utiliser le document SSM `AWSEC2-CreateVssSnapshot`.
- Le script appelle le document `AWSEC2-ManageVssIO` à deux reprises. La première fois avec le paramètre `Action` défini sur `Freeze`, ce qui suspend toutes les I/O sur les instances. La seconde fois, le paramètre `Action` est défini sur `Thaw`, ce qui force la reprise des I/O.
- N'essayez pas d'utiliser le `AWSEC2-ManageVssIO` document sans utiliser le script `CreateVssSnapshotAdvancedScript.ps1`. Le cadre VSS de Microsoft requiert que les actions `Freeze` et `Thaw` ne soient pas appelées à plus de dix secondes d'intervalle. L'appel manuel de ces actions sans le script risque de générer des erreurs.

Création d'instantanés EBS activés pour VSS à partir du document SSM **AWSEC2-ManageVssIO**

1. Téléchargez le fichier [CreateVssSnapshotAdvancedScript.zip](#) et extrayez le contenu du fichier.
2. Ouvrez `CreateVssSnapshotAdvancedScript.ps1` dans un éditeur de texte, modifiez l'exemple d'appel au bas du script avec un ID d'instance EC2 valide, une description de l'instantané et les valeurs de balise souhaitées, puis exécutez le script depuis PowerShell.

En cas de réussite, la commande complète automatiquement la liste des instantanés EBS avec les nouveaux instantanés. Vous pouvez localiser ces instantanés dans la liste des instantanés EBS en recherchant les balises que vous avez précisées ou en recherchant `AppConsistent`. Si l'exécution de la commande a échoué, consultez la sortie de commande pour en connaître les raisons. Si la commande a réussi mais que la sauvegarde d'un volume spécifique a échoué, vous pouvez résoudre l'échec dans la liste des volumes EBS.

Note

Pour automatiser les sauvegardes, vous pouvez créer une tâche de fenêtre de AWS Systems Manager maintenance qui utilise le `AWSEC2-VssInstallAndSnapshot` document. Pour

plus d'informations, consultez [Utilisation des fenêtres de maintenance \(console\)](#) dans le Guide de l'utilisateur AWS Systems Manager .

Créez des instantanés VSS à l'aide de AWS Backup

Vous pouvez créer une sauvegarde VSS lors de l'utilisation en AWS Backup activant VSS dans la console ou la CLI. Assurez-vous d'avoir respecté les [conditions préalables](#) avant de créer le plan de sauvegarde activé pour VSS. Pour plus d'informations sur cette fonction, consultez [Creating Windows VSS backups](#) dans le Guide du développeur AWS Backup .

Note

AWS Backup n'installe pas automatiquement le `AwsVssComponents` package sur votre instance. Vous devez effectuer une installation manuelle sur votre instance. Pour plus d'informations, consultez [Installation manuelle de composants VSS sur une instance](#).

Création d'instantanés VSS à l'aide d'Amazon Data Lifecycle Manager

Vous pouvez créer des instantanés VSS à l'aide d'Amazon Data Lifecycle Manager en activant les pré-scripts et les post-scripts dans vos politiques de cycle de vie des instantanés. Pour plus d'informations, consultez <https://docs.aws.amazon.com/ebs/latest/userguide/automate-app-consistent-backups.html>.

Note

Amazon Data Lifecycle Manager n'installe pas automatiquement le package `AwsVssComponents` sur votre instance. Vous devez effectuer une installation manuelle sur votre instance. Pour plus d'informations, consultez [Installation manuelle de composants VSS sur une instance](#).

Résoudre les problèmes liés aux instantanés EBS basés sur Windows VSS

Avant d'essayer d'autres étapes de résolution des problèmes, nous vous recommandons de vérifier les informations suivantes.

- Assurez-vous d'avoir respecté toutes les [Prérequis](#).
- Vérifiez que vous utilisez la dernière version de [Prise en charge de la version du système d'exploitation Windows](#) du package `AwsVssComponents` correspondant à votre système d'exploitation. Le problème que vous avez observé a peut-être été résolu dans les versions plus récentes.

Rubriques

- [Vérifier les fichiers journaux](#)
- [Collectez des journaux de diagnostic supplémentaires](#)
- [Utiliser VSS sur des instances avec un proxy configuré](#)
- [Erreur : « thaw pipe connection timed out », « error on thaw », « timeout waiting for VSS Freeze » ou autres erreurs de délai d'attente](#)
- [Erreur : impossible d'invoquer la méthode. L'invocation de méthodes n'est prise en charge que sur les types principaux dans ce mode de langue.](#)

Vérifier les fichiers journaux

Si vous rencontrez des problèmes ou recevez des messages d'erreur lorsque vous créez des instantanés EBS compatibles VSS, vous pouvez consulter le résultat de la commande dans la console Systems Manager.

Pour les documents Systems Manager qui créent des instantanés VSS, vous pouvez définir le `CollectDiagnosticLogs` paramètre sur « True » au moment de l'exécution. Lorsque le `CollectDiagnosticLogs` paramètre est défini sur True « », VSS collecte des journaux supplémentaires pour faciliter le débogage. Pour plus d'informations, consultez [Collectez des journaux de diagnostic supplémentaires](#).

Si vous collectez des journaux de diagnostic, le document Systems Manager les stocke sur votre instance à l'emplacement suivant : `C:\ProgramData\Amazon\AwsVss\Logs\timestamp.zip`. La valeur par défaut du `CollectDiagnosticLogs` paramètre est « False ».

Note

Pour obtenir de l'aide supplémentaire pour le débogage, vous pouvez envoyer le `.zip` fichier à AWS Support.

Les journaux supplémentaires suivants sont disponibles, que vous recueilliez des journaux de diagnostic ou non :

- %ProgramData%\Amazon\SSM\InstanceData*InstanceID*\document\orchestration*SSMCommandID*\awsrunPowerShellScript\runPowerShellScript\stdout
- %ProgramData%\Amazon\SSM\InstanceData*InstanceID*\document\orchestration*SSMCommandID*\awsrunPowerShellScript\runPowerShellScript\stderr

Vous pouvez également ouvrir l'application Observateur d'événements de Windows et sélectionner Journaux Windows, Application pour afficher les journaux supplémentaires. Pour afficher les événements spécifiquement du fournisseur VSS Windows EC2 et du Service de cliché instantané des volumes, filtrez par source avec les termes **Ec2VssSoftwareProvider** et **VSS**.

Si vous utilisez Systems Manager avec des points de terminaison VPC et que l'action de l'[SendCommand](#) API Systems Manager (Exécuter la commande dans la console) a échoué, vérifiez que vous avez correctement configuré le point de terminaison suivant : com.amazonaws.*région*.ec2.

Si le point de terminaison Amazon EC2 n'est pas défini, l'appel pour énumérer les volumes EBS attachés échoue, ce qui entraîne l'échec de la commande Systems Manager. Pour plus d'informations sur la configuration de points de terminaison d'un VPC avec Systems Manager, consultez [Create a Virtual Private Cloud Endpoint](#) (Créer un point de terminaison VPC) dans le Guide de l'utilisateur AWS Systems Manager .

Collectez des journaux de diagnostic supplémentaires

Pour collecter des journaux de diagnostic supplémentaires lorsque vous utilisez la commande d'envoi de Systems Manager pour exécuter le document instantané VSS, définissez le paramètre CollectDiagnosticLogs d'entrée sur « True » lors de l'exécution. Nous vous recommandons de définir ce paramètre sur « True » lors de la résolution des problèmes.

Pour voir un exemple de ligne de commande, sélectionnez l'un des onglets suivants.

AWS CLI

L'exemple suivant exécute le document AWSEC2-CreateVssSnapshot Systems Manager dans le AWS CLI :

```
aws ssm send-command \
```

```
--document-name "AWSEC2-CreateVssSnapshot" \  
--instance-ids "i-1234567890abcdef0" \  
--parameters '{"description":["Example - create diagnostic logs at  
runtime."], "tags":["Key=tag_name, Value=tag_value"], "CollectDiagnosticLogs":  
["True"]}'
```

PowerShell

L'exemple suivant exécute le document AWSEC2-CreateVssSnapshot Systems Manager dans PowerShell :

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId  
"i-1234567890abcdef0" -Parameter @{'description'='Example - create diagnostic logs  
at runtime.'; 'tags'='Key=tag_name, Value=tag_value'; 'CollectDiagnosticLogs'='True'}
```

Utiliser VSS sur des instances avec un proxy configuré

Si vous rencontrez des problèmes lors de la création d'instantanés EBS compatibles avec VSS sur des instances qui utilisent un proxy pour atteindre les points de terminaison EC2, assurez-vous que :

- Le proxy est configuré de telle sorte que les points de terminaison du service EC2 de la région et de l'IMDS de l'instance soient accessibles en AWS Tools for Windows PowerShell exécutant le code SYSTEM.
- AwsVssComponents version 2.0.1 ou ultérieure installée. Depuis AwsVssComponents version 2.0.1, le fournisseur VSS EC2 prend en charge l'utilisation du proxy WinHTTP configuré sur le système. Pour plus d'informations sur la configuration du proxy WinHTTP, consultez la section [Commandes Netsh pour Windows Hypertext Transfer Protocol \(WINHTTP\)](#) (français non garanti) sur le site web de Microsoft.

Erreur : « thaw pipe connection timed out », « error on thaw », « timeout waiting for VSS Freeze » ou autres erreurs de délai d'attente

Le fournisseur VSS Windows EC2 peut expirer en raison de l'activité ou des services sur l'instance empêchant les instantanés compatibles VSS de poursuivre leur activité en temps opportun. Le framework VSS Windows fournit une fenêtre de 10 secondes non configurable pendant laquelle la communication avec le système de fichiers est suspendue. Pendant ce temps, AWSEC2-CreateVssSnapshot crée des instantanés de vos volumes.

Les problèmes suivants peuvent amener le fournisseur VSS Windows EC2 à rencontrer des limites de temps au cours d'un instantané :

- I/O excessives vers un volume
- Réactivité lente de l'API EC2 sur l'instance
- Volumes fragmentés
- Incompatibilité avec certains logiciels antivirus
- Problèmes avec un enregistreur d'application VSS
- Lorsque la journalisation des modules est activée pour un grand nombre de PowerShell modules, cela peut entraîner un ralentissement de l'exécution PowerShell des scripts

La plupart des délais d'expiration qui se produisent lorsque vous exécutez le document de commande `AWSEC2-CreateVssSnapshot` sont liés au fait que la charge de travail sur l'instance est trop élevée au moment de la sauvegarde. Pour vous aider à créer un instantané avec succès, vous pouvez procéder comme suit :

- Réessayez la commande `AWSEC2-CreateVssSnapshot` pour voir si la tentative d'instantané réussit. Si une nouvelle tentative réussit dans certains cas, la réduction de la charge de l'instance peut favoriser la réussite des instantanés.
- Patientez le temps que la charge globale sur l'instance diminue, puis réessayez la commande `AWSEC2-CreateVssSnapshot`. Vous pouvez également essayer des instantanés lorsque vous savez que l'instance est soumise à une faible contrainte.
- Essayez des instantanés VSS lorsque le logiciel antivirus sur le système est désactivé. Si cela résout le problème, reportez-vous aux instructions du logiciel antivirus et configurez celui-ci afin qu'il autorise les instantanés VSS.
- S'il y a un volume élevé d'appels d'API Amazon EC2 dans votre compte au sein de la même région où vous exécutez un instantané, la limitation de l'API peut retarder les opérations de l'instantané. Pour réduire l'impact de la limitation, utilisez le dernier package `AwsVssComponents` (version 2.1.0 et supérieure, avec les autorisations préalables requises). Ce package utilise l'action `CreateSnapshots` de l'API EC2 pour réduire le nombre d'actions de mutation telles que la création et le balisage d'instantanés par volume.
- Si plusieurs scripts de commande `AWSEC2-CreateVssSnapshot` s'exécutent en même temps, vous pouvez suivre les étapes suivantes pour réduire les problèmes de simultanéité.
 - Envisagez de planifier des instantanés pendant les périodes de faible activité des API.

- Si vous exécutez le script de commande Run Command dans la console Systems Manager (ou SendCommand dans l'API), vous pouvez utiliser les contrôles de débit de Systems Manager pour réduire la simultanéité.

Vous pouvez également utiliser les contrôles de débit de Systems Manager pour réduire la simultanéité des services tels AWS Backup que ceux qui utilisent Systems Manager pour exécuter le script de commande.

- Exécutez la commande `vssadmin list writers` dans un shell et voyez si celle-ci signale des erreurs dans le champ Last error pour tous les enregistreurs sur le système. Si des enregistreurs signalent une erreur time out, vous pouvez éventuellement réessayer de créer des instantanés lorsque l'instance sera moins chargée.
- Lorsque vous utilisez des types d'instances plus petits tels que `t2` / `t3` / `t3a.nano` ou `t2` / `t3` / `t3a.micro`, des délais d'expiration dus à des contraintes de mémoire et de processeur peuvent survenir. Les actions suivantes peuvent contribuer à réduire les problèmes de délai d'expiration.
 - Essayez de fermer les applications utilisant la mémoire ou le processeur de manière intensive avant de prendre des instantanés.
 - Essayez de prendre des instantanés pendant les périodes de faible activité de l'instance.

Erreur : impossible d'invoquer la méthode. L'invocation de méthodes n'est prise en charge que sur les types principaux dans ce mode de langue.

Vous rencontrerez cette erreur lorsque le mode de PowerShell langue n'est pas défini sur `FullLanguage`. Les documents `AWSEC2-CreateVssSnapshot` et `AWSEC2-ManageVssIo` SSM doivent PowerShell être configurés en `FullLanguage` mode.

Pour vérifier le mode de langue, exécutez la commande suivante sur l'instance dans une PowerShell console :

```
$ExecutionContext.SessionState.LanguageMode
```

Pour plus d'informations sur les modes de langue, veuillez consulter la rubrique [about_Language_Modes](#) dans la documentation Microsoft.

Restaurer des volumes à partir d'instantanés EBS compatibles avec VSS

Vous pouvez utiliser le script `RestoreVssSnapshotSampleScript.ps1` pour restaurer des volumes sur une instance à partir d'instantanés EBS activés pour VSS. Ce script effectue les tâches suivantes :

- Arrête une instance
- Supprime tous les disques existants de l'instance (à l'exception du volume de démarrage, s'il a été exclu)
- Crée de nouveaux volumes à partir des instantanés
- Attache les volumes à l'instance en utilisant la balise d'ID de périphérique sur l'instantané
- Redémarre l'instance

Important

Le script suivant détache tous les volumes attachés à une instance, puis crée de nouveaux volumes à partir d'un instantané. Vérifiez que vous avez correctement sauvegardé l'instance. Les anciens volumes ne sont pas supprimés. Si vous le souhaitez, vous pouvez modifier le script afin de supprimer les anciens volumes.

Restauration de volumes à partir d'instantanés EBS activés pour VSS

1. Téléchargez le fichier [RestoreVssSnapshotSampleScript.zip](#) et extrayez le contenu du fichier.
2. Ouvrez `RestoreVssSnapshotSampleScript.ps1` dans un éditeur de texte et modifiez l'exemple d'appel au bas du script avec un ID d'instance EC2 et un ID de snapshot EBS valides, puis exécutez le script depuis PowerShell

AWS Historique des versions de la solution VSS

Rubriques

- [AwsVssComponents versions du package](#)
- [Prise en charge de la version du système d'exploitation Windows](#)

AwsVssComponents versions du package

Le tableau suivant décrit les versions publiées du package de composants AWS VSS.

Version	Détails	Date de publication
2.3.2	Correction d'un cas où l'enregistrement du fournisseur VSS n'était pas supprimé lors de la désinstallation.	9 mai 2024
2.3.1	Ajout d'une nouvelle balise par défaut <code>AwsVssConfig</code> pour identifier les instantanés et les AMI créés par AWS VSS.	7 mars 2024
2.2.1	<ul style="list-style-type: none">• Ajout du support pour l'utilisation de l'<code>DescribeInstanceAttribute</code> API.• Correctifs de bogues et améliorations de fiabilité.• Support obsolète pour Windows Server 2012 et 2012 R2. AWS L'installation des composants VSS version 2.2.1 sur Windows Server 2012 et 2012 R2 échouera. AWS La version 2.1.0 des composants VSS est la dernière version compatible avec Windows Server 2012 et 2012 R2.	18 janvier 2024
2.1.0	Ajout du support pour l'utilisation de l' <code>CreateSnapshots</code> API.	6 novembre 2023
2.0.1	Ajout de la prise en charge de l'utilisation des paramètres du proxy WinHTTP.	26 octobre 2023
2.0.0	Fonctionnalité ajoutée au composant AWS VSS pour créer des instantanés et des AMI, ce qui permet la compatibilité avec les fonctionnalités de journalisation des PowerShell modules, de journalisation des blocs de script et de transcription.	28 avril 2023

Version	Détails	Date de publication
1.3.2.0	Correction d'un cas où l'échec de l'installation n'était pas signalé correctement.	10 mai 2022
1.3.1.0	<ul style="list-style-type: none">• Correction des instantanés échouant sur les contrôleurs de domaine en relation avec une erreur de journalisation de l'enregistreur NTDS VSS.• Correction d'une erreur de l'agent VSS lors de la désinstallation du fournisseur VSS version 1.0.	6 février 2020
1.3.00	<ul style="list-style-type: none">• Amélioration de la journalisation par la réduction du niveau de détail indésirable.• Correction des problèmes de régionalisation lors de l'installation.• Correction des codes de retour pour certaines conditions d'erreur d'enregistrement du fournisseur.• Correction de divers problèmes d'installation.	19 mars 2019
1.2.00	<ul style="list-style-type: none">• Ajout de paramètres de ligne de commande -nw (no-writers) et -copy (copy-only) à l'agent.• Correction EventLog d'erreurs causées par des appels d'allocation de mémoire incorrects.	le 15 novembre 2018
1.1	Correction de composants AWS VSS qui n'étaient pas utilisés correctement en tant que fournisseur de sauvegarde et de restauration Windows par défaut.	12 décembre 2017

Version	Détails	Date de publication
1.0	Première version.	le 20 novembre 2017

Prise en charge de la version du système d'exploitation Windows

Le tableau suivant indique les versions de solution AWS VSS que vous devez exécuter sur chaque version de Windows Server sur Amazon EC2.

Version Windows Server	AwsVssComponents version	AWSEC2-nom de VssInstal lAndSnaps hot version	AWSEC2-nom de CreateVss Snapshot version	AWSEC2-Nom de la version ManageVss IO
Windows Server 2022	default	default	default	default
Windows Server 2019	default	default	default	default
Windows Server 2016	default	default	default	default
Windows Server 2012 R2	2.1.0	non pris en charge	2012R2	2012R2
Windows Server 2012 R2	2.1.0	non pris en charge	2012R2	2012R2

Version Windows Server	AwsVssComponents version	AWSEC2-nom de VssInstal lAndSnaps hot version	AWSEC2-nom de CreateVss Snapshot version	AWSEC2-Nom de la version ManageVss IO
Windows S	1.3.1.0	non pris en charge	2008R2	2008R2

Prévention de l'écriture déchirée pour les instances Linux

Note

La prévention de l'écriture déchirée est prise en charge uniquement avec les instances Linux.

La prévention de l'écriture déchirée est une fonctionnalité de stockage par blocs conçue AWS pour améliorer les performances de vos charges de travail de base de données relationnelles intensives en E/S et réduire la latence sans affecter négativement la résilience des données. Les bases de données relationnelles qui utilisent InnoDB ou XtraDB comme moteur de base de données, telles que MySQL et MariaDB, bénéficieront d'une protection contre les écritures déchirées.

En règle générale, les bases de données relationnelles qui utilisent des pages plus grandes que l'atomicité en cas de panne du périphérique de stockage utilisent des mécanismes de journalisation de données pour se protéger contre les écritures déchirées. MariaDB et MySQL utilisent un fichier tampon à double écriture pour journaliser les données avant de les écrire dans des tables de données. En cas d'écritures incomplètes ou déchirées, à la suite d'une panne du système d'exploitation ou d'une panne de courant pendant les transactions d'écriture, la base de données peut récupérer les données de la mémoire tampon à double écriture. La surcharge d'E/S supplémentaire associée à l'écriture dans la mémoire tampon à double écriture a un impact sur les performances de la base de données et la latence des applications. De plus, elle réduit le nombre de transactions pouvant être traitées par seconde. Pour plus d'informations sur la mémoire tampon à double écriture, veuillez consulter la documentation [MariaDB](#) et [MySQL](#).

Grâce à la prévention des écritures déchirées, les données sont écrites dans la mémoire dans le cadre de transactions d'écriture tout ou rien, ce qui évite de devoir utiliser la mémoire tampon à double écriture. Cela empêche l'écriture de données partielles ou déchirées dans le stockage en cas de panne du système d'exploitation ou de panne de courant lors des transactions d'écriture. Le nombre de transactions traitées par seconde peut être augmenté jusqu'à 30 % et la latence d'écriture peut être réduite jusqu'à 50 %, sans compromettre la résilience de vos charges de travail.

Tarification

L'utilisation de la solution de prévention des écritures déchirées est disponible sans coûts supplémentaires.

Tailles de bloc et alignements des limites de blocs pris en charge

La prévention des écritures déchirées prend en charge les opérations d'écriture pour des blocs de données de 4 Kio, 8 Kio et 16 Kio. L'adresse de bloc logique (LBA) de début du bloc de données doit être alignée sur la taille limite de bloc respective de 4 Kio, 8 Kio ou 16 Kio. Par exemple, pour les opérations d'écriture de 16 Kio, le LBA de départ du bloc de données doit être aligné sur une taille de limite de bloc de 16 Kio.

Le tableau suivant présente la prise en charge des différents types de stockage et d'instance.

	Blocs de 4 Kio	Blocs de 8 Kio	Blocs de 16 Kio
Volumes de stockage d'instances	Tous les volumes de stockage d'instances NVMe attachés aux instances de la famille I de génération actuelle.	Instances i4i, iM4GN et IS4gen prises en charge par le SSD Nitro. AWS	
Volumes Amazon EBS	Tous les volumes Amazon EBS attachés à des instances basées sur le système AWS Nitro .		

Pour vérifier si votre instance et votre volume prennent en charge la prévention des écritures déchirées, adressez une requête afin de vérifier si l'instance prend en charge la prévention des écritures déchirées et fournissez d'autres informations, telles que les tailles de blocs et de limites

prises en charge. Pour plus d'informations, consultez [Vérifier la prise en charge et la configuration de la prévention des écritures déchirées](#).

Prérequis

Pour que la prévention des écritures déchirées fonctionne correctement, une opération d'E/S doit respecter les exigences de taille, d'alignement et de limites, telles que spécifiées dans les champs NTWPU, NTWGU et NTWBU. Vous devez configurer votre système d'exploitation pour vous assurer que le sous-système de stockage spécifique (système de fichiers, LVM, RAID, etc.) ne modifie pas les propriétés d'E/S sur la pile de stockage, y compris les fusions de blocs, les divisions ou la relocalisation d'adresses de blocs, avant de le soumettre au périphérique.

La prévention des écritures déchirées a été testée avec la configuration suivante :

- Type d'instance et type de stockage qui prennent en charge la taille de bloc requise.
- Amazon Linux 2 avec la version du noyau 5.10 ou version ultérieure.
- ext4 avec `bigalloc` activé et une taille de cluster de 16 Kio, ainsi que les utilitaires ext4 les plus récents (`e2fsprogs 1.46.5` ou version ultérieure).
- Mode d'accès aux fichiers `O_DIRECT` pour contourner le cache tampon du noyau Linux.

Note

Vous n'avez pas besoin de désactiver la fusion d'E/S pour les charges de travail MySQL et MariaDB.

Vérifier la prise en charge et la configuration de la prévention des écritures déchirées

Pour vérifier si votre instance et votre volume prennent en charge la prévention des écritures déchirées et pour consulter les données propres au fournisseur de l'espace de noms NVMe contenant des informations relatives à la prévention des écritures déchirées, utilisez la commande suivante.

```
$ sudo nvme id-ns -v device_name
```

Note

La commande renvoie les informations propres au fournisseur en hexadécimal avec interprétation ASCII. Il se peut que vous deviez intégrer à vos applications un outil similaire à `esbnvme-id` capable de lire et d'analyser les résultats.

Par exemple, la commande suivante renvoie les données propres au fournisseur de l'espace de noms NVMe qui contiennent des informations de prévention des écritures déchirées pour `/dev/nvme1n1`.

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Si votre instance et votre volume prennent en charge la prévention de l'écriture déchirée, ils renvoient les informations de prévention de l'écriture AWS déchirée suivantes dans les données spécifiques au fournisseur de l'espace de noms NVMe.

Note

Les octets du tableau suivant représentent le décalage en octets par rapport au début des données propres au fournisseur de l'espace de noms NVMe.

Octets	Description
0:31	Le nom du point de montage de l'attachement du périphérique, par exemple <code>/dev/xvda</code> . Vous l'indiquez lors de la demande d'attachement de volume et il peut être utilisé par l'instance Amazon EC2 pour créer un lien symbolique vers le périphérique de stockage en mode bloc NVMe (<code>nvmeXn1</code>).
32:63	ID du volume. Par exemple, <code>vol01234567890abcdef</code> . Ce champ peut être utilisé pour mapper le périphérique NVMe au volume attaché.
64:255	Réservé pour un usage futur.
256:257	Taille de l'unité de prévention des écritures déchirées dans l'espace de noms (NTWPU). Ce champ indique la taille propre à l'espace de noms

Octets	Description
	de l'opération d'écriture dont l'écriture est garantie de manière atomique sur la NVM en cas de panne de courant ou de condition d'erreur. Ce champ est spécifié dans des blocs logiques représentés par des valeurs basées sur zéro.
258:259	Taille de granularité de la prévention des écritures déchirées de l'espace de noms (NTWPG). Ce champ indique les incréments de la taille propre à l'espace de noms inférieure à NTWPU de l'opération d'écriture dont l'écriture est garantie de manière atomique sur la NVM en cas de panne ou de condition d'erreur. C'est-à-dire que la taille doit être $NTWPG * n \leq NTWPU$, où n est un entier positif. Le décalage LBA de l'opération d'écriture doit également être aligné sur ce champ. Ce champ est spécifié dans des blocs logiques représentés par des valeurs basées sur zéro.
260:263	Taille de la limite de prévention des écritures déchirées dans l'espace de noms (NTWPB). Ce champ indique la taille de la limite atomique pour cet espace de noms pour la valeur NTWPU. Il n'est pas garanti que les écritures dans cet espace de nom qui traversent les frontières atomiques sont écrites de manière atomique sur la NVM en cas de panne de courant ou de condition d'erreur. Une valeur de 0h indique qu'il n'existe pas de limites atomiques pour les conditions de panne ou d'erreur. Toutes les autres valeurs indiquent une taille en termes de blocs logiques utilisant le même codage que le champ NTWPU.

Configuration de votre pile logicielle pour empêcher les écritures déchirées

La prévention des écritures déchirées est activée par défaut sur les [types d'instances pris en charge avec des volumes pris en charge](#). Vous n'avez pas besoin d'activer de paramètres supplémentaires pour activer la prévention des écritures déchirées sur votre volume ou votre instance.

Note

Il n'y a aucun impact sur les performances quant aux charges de travail qui ne prennent pas en charge la prévention des écritures déchirées. Vous n'avez pas besoin d'apporter des modifications pour ces charges de travail.

Les charges de travail qui prennent en charge la prévention des erreurs d'écriture, mais qui ne sont pas configurées pour l'utiliser, continuent à utiliser la mémoire tampon à double écriture et ne bénéficient d'aucun avantage en termes de performances.

Pour configurer votre pile logicielle MySQL ou MariaDB afin de désactiver le tampon de double écriture et d'utiliser la prévention des écritures déchirées, procédez comme suit :

1. Configurez votre volume pour utiliser le système de fichiers ext4 avec l' `BigAlloc` option et définissez la taille du cluster sur 4 KiB, 8 KiB ou 16 KiB. L'utilisation `BigAlloc` d'une taille de cluster de 4 KiB, 8 KiB ou 16 KiB garantit que le système de fichiers alloue les fichiers conformément à la limite correspondante.

```
$ mkfs.ext4 -O bigalloc -C 4096/8192/16384 device_name
```

Note

Pour MySQL et MariaDB, vous devez utiliser `-C 16384` pour faire correspondre la taille de page de la base de données. La définition de la granularité d'allocation sur une valeur autre qu'un multiple de la taille de page peut entraîner des allocations qui peuvent ne pas correspondre aux limites de prévention des écritures déchirées du périphérique de stockage.

Par exemple :

```
$ mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
```

2. Configurez InnoDB pour utiliser la méthode de vidage `0_DIRECT` et désactivez la double écriture d'InnoDB. Utilisez l'éditeur de texte de votre choix pour ouvrir `/etc/my.cnf` et mettez à jour les paramètres `innodb_flush_method` et `innodb_doublewrite` comme suit :

```
innodb_flush_method=0_DIRECT
```

```
innodb_doublewrite=0
```

Important

Si vous utilisez Logical Volume Manager (LVM) ou une autre couche de virtualisation du stockage, assurez-vous que les décalages de départ des volumes sont alignés sur des multiples de 16 Kio. Ceci est relatif au stockage NVMe sous-jacent pour tenir compte des entêtes de métadonnées et des superblocs utilisés par la couche de virtualisation du stockage. Si vous ajoutez un décalage au volume physique de la LVM, cela peut entraîner un défaut d'alignement entre les allocations du système de fichiers et les décalages du périphérique NVMe, ce qui annulerait la prévention des écritures déchirées. Pour plus d'informations, veuillez consulter `--dataalignmentoffset` dans la [page Amazon Linux](#).

Ressources et balises

Amazon EC2 fournit différentes ressources que vous pouvez créer et utiliser. Certaines de ces ressources incluent des images, des instances, des volumes et des instantanés. Lorsque vous créez une ressource, nous lui affectons un ID de ressource unique.

Certaines ressources peuvent être balisées avec des valeurs que vous définissez pour mieux les organiser et les identifier.

Les rubriques suivantes décrivent les ressources et les balises, et expliquent comment les utiliser.

Table des matières

- [Corbeille](#)
- [Emplacements des ressources](#)
- [ID de ressource](#)
- [Lister et filtrer vos ressources](#)
- [Amazon EC2 Global View \(Amazon EC2 Global View\)](#)
- [Baliser vos ressources Amazon EC2](#)
- [Quotas de service Amazon EC2](#)

Corbeille

La corbeille est une fonction de récupération de données qui vous permet de restaurer des instantanés Amazon EBS et des AMI basées sur EBS supprimés accidentellement. Lorsque vous utilisez la corbeille, si vos ressources sont supprimées, elles sont retenues dans la corbeille pendant une période spécifiée avant leur suppression définitive.

Vous pouvez restaurer une ressource à partir de la corbeille à tout moment avant l'expiration de sa période de rétention. Une fois que vous avez restauré une ressource à partir de la corbeille, elle est supprimée de la corbeille et vous pouvez l'utiliser de la même manière que n'importe quelle autre ressource de ce type sur votre compte. Si la période de rétention expire et que la ressource n'est pas restaurée, elle est définitivement supprimée de la corbeille et n'est plus disponible pour restauration.

L'utilisation de la corbeille aide à garantir la continuité métier en protégeant vos données métier critiques contre toute suppression accidentelle.

Rubriques

- [Fonctionnement](#)
- [Ressources prises en charge](#)
- [Considérations](#)
- [Quotas](#)
- [Services connexes](#)
- [Tarification](#)
- [Autorisations IAM requises](#)
- [Utiliser des règles de rétention](#)
- [Utiliser des ressources dans la corbeille](#)
- [Surveiller la corbeille](#)

Fonctionnement

Pour activer et utiliser la corbeille, vous devez créer des règles de conservation dans les AWS régions dans lesquelles vous souhaitez protéger vos ressources. Les règles de rétention précisent :

- Le type de ressource que vous souhaitez protéger.
- Les ressources que vous souhaitez retenir dans la corbeille lorsqu'elles sont supprimées.
- La période de rétention pendant laquelle les ressources doivent être retenues dans la corbeille avant d'être définitivement supprimées.

Avec la Corbeille, vous pouvez créer deux types de règles de rétention :

- Règles de rétention au niveau des identifications : une règle de rétention au niveau des identifications utilise des identifications de ressources pour identifier les ressources qui doivent être retenues dans la corbeille. Pour chaque règle de rétention, vous spécifiez une ou plusieurs paires clé-valeur d'identification. Les ressources du type spécifique qui sont étiquetées avec au moins une des paires clé-valeur d'identification qui sont spécifiées dans la règle de rétention sont automatiquement retenues dans la corbeille lors de leur suppression. Utilisez ce type de règle de rétention si vous souhaitez protéger des ressources spécifiques de votre compte en fonction de leurs identifications.
- Règles de rétention au niveau de la Région : aucune identification de ressource n'est spécifiée dans une règle de rétention au niveau de la Région. Elle s'applique à toutes les ressources du type spécifié dans la Région dans laquelle la règle est créée, même si elles ne sont pas étiquetées.

Utilisez ce type de règle de rétention si vous souhaitez protéger toutes les ressources d'un type spécifique dans une Région spécifique.

Lorsqu'une ressource se trouve dans la corbeille, il est possible de la restaurer à tout moment.

La ressource reste dans la corbeille jusqu'à ce que l'un des événements suivants se produise :

- Vous le restaurez manuellement pour l'utiliser. Lorsque vous restaurez une ressource à partir de la corbeille, celle-ci est supprimée de la corbeille et elle devient immédiatement disponible pour être utilisée. Vous pouvez utiliser les ressources restaurées de la même manière que n'importe quelle autre ressource de ce type dans votre compte.
- La période de rétention expire. Si la période de rétention expire et que la ressource n'a pas été restaurée à partir de la corbeille, elle est définitivement supprimée de la corbeille et ne peut plus être affichée ou restaurée.

Ressources prises en charge

La corbeille prend en charge les types de ressources suivants :

- Instantanés Amazon EBS

Important

Les règles de conservation de la corbeille s'appliquent également aux instantanés archivés dans le niveau de stockage des archives. Si vous supprimez un instantané archivé qui correspond à une règle de conservation, cet instantané est conservé dans la corbeille pendant la période définie dans la règle de conservation. Les instantanés archivés sont facturés au tarif des instantanés archivés lorsqu'ils se trouvent dans la corbeille.

- Amazon Machine Images (AMI) basées sur Amazon EBS

Note

Les règles de conservation s'appliquent également aux AMI désactivées.

Considérations

Les points suivants s'appliquent lors de l'utilisation de la corbeille et des règles de rétention.

Considérations d'ordre général

-  **Important**
Lorsque vous créez votre première règle de rétention, la règle peut prendre jusqu'à 30 minutes pour s'activer et commencer à retenir les ressources. Après avoir créé la première règle de rétention, les règles de rétention suivantes deviennent actives et commencent à retenir les ressources presque immédiatement.
- Si une ressource correspond à plus d'une règle de conservation lors de la suppression, la règle de conservation ayant la période de conservation la plus longue a la priorité.
- Vous ne pouvez pas supprimer manuellement une ressource de la corbeille. La ressource sera supprimée automatiquement à l'expiration de sa période de rétention.
- Lorsqu'une ressource se trouve dans la corbeille, vous pouvez uniquement l'afficher, la restaurer ou modifier ses identifications. Pour utiliser la ressource d'une autre manière, vous devez d'abord la restaurer.
- Si une ressource Service AWS, telle que AWS Backup ou Amazon Data Lifecycle Manager, supprime une ressource correspondant à une règle de conservation, cette ressource est automatiquement conservée par Recycle Bin.
- Lorsqu'une ressource est envoyée à la corbeille, l'identification de génération système suivante est affectée à la ressource :
 - Clé d'identification : `aws:recycle-bin:resource-in-bin`
 - Valeur d'identification : `true`

Vous ne pouvez pas modifier ou supprimer manuellement cette identification. Lorsque la ressource est restaurée à partir de la corbeille, l'identification est automatiquement supprimée.

Considérations relatives aux instantanés

-  **Important**
Si vous disposez de règles de rétention pour les AMI et pour leurs instantanés associés, faites en sorte que la période de rétention des instantanés soit identique ou plus longue

que la période de rétention des AMI. Cela garantit que la corbeille ne supprime pas les instantanés associés à une AMI avant de supprimer l'AMI elle-même, car cela rendrait l'AMI irrécupérable.

- Si la restauration rapide d'instantané est activée pour un instantané lorsqu'il est supprimé, elle est automatiquement désactivée peu de temps après l'envoi de l'instantané dans la corbeille.
 - Si vous restaurez l'instantané avant que la restauration rapide d'instantané ne soit désactivée pour l'instantané, elle reste activée.
 - Si vous restaurez l'instantané, une fois que la restauration d'instantané rapide a été désactivée, elle reste désactivée. Si nécessaire, vous devez réactiver manuellement la restauration rapide d'instantané.
- Si un instantané est partagé lors de sa suppression, le partage est automatiquement annulé lorsqu'il est envoyé à la corbeille. Si vous restaurez l'instantané, toutes les autorisations de partage précédentes sont automatiquement restaurées.
- Si un instantané créé par un autre AWS service, par exemple, AWS Backup est envoyé à la corbeille et que vous restaurez ultérieurement cet instantané à partir de la corbeille, il n'est plus géré par le AWS service qui l'a créé. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.

Considérations relatives aux AMI

- Seules les AMI d'Amazon EBS sont prises en charge.

Important

Si vous disposez de règles de rétention pour les AMI et pour leurs instantanés associés, faites en sorte que la période de rétention des instantanés soit identique ou plus longue que la période de rétention des AMI. Cela garantit que la corbeille ne supprime pas les instantanés associés à une AMI avant de supprimer l'AMI elle-même, car cela rendrait l'AMI irrécupérable.

- Si une AMI est partagée lors de sa suppression, le partage est automatiquement annulé lorsqu'elle est envoyée à la corbeille. Si vous restaurez l'AMI, toutes les autorisations de partage précédentes sont automatiquement restaurées.
- Avant de pouvoir restaurer une AMI à partir de la corbeille, vous devez d'abord restaurer tous les instantanés associés à partir de la corbeille et vous assurer qu'ils se trouvent à l'état `available`.

- Si les instantanés associés à l'AMI sont supprimés de la corbeille, l'AMI n'est plus récupérable. L'AMI sera supprimée à l'expiration de la période de rétention.
- Si une AMI créée par un autre AWS service, tel que AWS Backup, est envoyée à la corbeille et que vous restaurez ultérieurement cette AMI à partir de la corbeille, elle n'est plus gérée par le AWS service qui l'a créée. Vous devez supprimer manuellement l'AMI si elle n'est plus nécessaire.

Considérations relatives aux politiques d'instantanés Amazon Data Lifecycle Manager

- Si Amazon Data Lifecycle Manager supprime un instantané qui correspond à une règle de conservation, cet instantané est automatiquement conservé par la corbeille.
- Si Amazon Data Lifecycle Manager supprime un instantané et l'envoie à la corbeille lorsque le seuil de rétention de la politique est atteint, et que vous restaurez manuellement l'instantané à partir de la corbeille, vous devez supprimer manuellement cet instantané s'il n'est plus nécessaire. Amazon Data Lifecycle Manager ne gèrera plus l'instantané.
- Si vous supprimez manuellement un instantané créé par une politique et que cet instantané se trouve dans la corbeille lorsque le seuil de rétention de la politique est atteint, Amazon Data Lifecycle Manager ne supprime pas l'instantané. Amazon Data Lifecycle Manager ne gère pas les instantanés lorsqu'ils sont stockés dans la corbeille.

Si l'instantané est restauré à partir de la corbeille avant que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager supprime l'instantané lorsque le seuil de rétention de la politique est atteint.

Si l'instantané est restauré à partir de la corbeille après que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager ne supprime plus l'instantané. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.

Considérations relatives à la AWS sauvegarde

- Si AWS Backup supprime un instantané conforme à une règle de conservation, cet instantané est automatiquement conservé par Recycle Bin.

Considérations relatives aux instantanés archivés

- Les règles de conservation de la corbeille s'appliquent également aux instantanés archivés dans le niveau de stockage des archives. Si vous supprimez un instantané archivé qui correspond à

une règle de conservation, cet instantané est conservé dans la corbeille pendant la période définie dans la règle de conservation.

Les instantanés archivés sont facturés au tarif des instantanés archivés lorsqu'ils se trouvent dans la corbeille.

Si une règle de conservation supprime un instantané archivé de la corbeille avant la période d'archivage minimale de 90 jours, vous êtes facturé pour les jours restants. Pour plus d'informations, consultez la section [Tarification et facturation des instantanés archivés](#) dans le guide de l'utilisateur Amazon EBS.

Pour utiliser un instantané archivé qui se trouve dans la corbeille, vous devez d'abord récupérer l'instantané depuis la corbeille, puis le restaurer du niveau d'archivage au niveau standard.

Quotas

Les quotas suivants s'appliquent à la corbeille.

Quota	Quota par défaut			
Règles de rétention par région	250			
Paires clé-valeur d'identification par règle de rétention	50			

Services connexes

La corbeille fonctionne avec les services suivants :

- AWS CloudTrail : permet d'enregistrer les événements qui se produisent dans la corbeille. Pour plus d'informations, consultez [Surveillez l'utilisation de la corbeille AWS CloudTrail](#).

Tarification

Les ressources de la corbeille sont facturées à leur tarif standard. Il n'y a pas de facturation supplémentaire pour l'utilisation de la corbeille et des règles de rétention. Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

Note

Certaines ressources peuvent encore apparaître dans la console de la corbeille ou dans la sortie de l'API AWS CLI et pendant une courte période après l'expiration de leur période de conservation et leur suppression définitive. Ces ressources ne vous sont pas facturées. La facturation s'arrête dès que la période de rétention expire.

Vous pouvez utiliser les balises de répartition des coûts AWS générées suivantes à des fins de suivi et de répartition des coûts lors de l'utilisation AWS Billing and Cost Management.

- Clé : `aws:recycle-bin:resource-in-bin`
- Valeur : `true`

Pour plus d'informations, veuillez consulter la section [Balises de répartition des coûts générées par AWS](#) dans le Guide de l'utilisateur AWS Billing and Cost Management .

Autorisations IAM requises

Par défaut, les utilisateurs ne sont pas autorisés à utiliser la corbeille, les règles de rétention ou les ressources contenues dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Rubriques

- [Autorisations pour utiliser la corbeille et les règles de rétention](#)
- [Autorisations pour utiliser des ressources dans la corbeille](#)
- [Clés de condition pour la corbeille](#)

Autorisations pour utiliser la corbeille et les règles de rétention

Pour utiliser la corbeille et les règles de rétention, les utilisateurs ont besoin des autorisations suivantes.

- `rbin:CreateRule`
- `rbin:UpdateRule`
- `rbin:GetRule`
- `rbin:ListRules`
- `rbin>DeleteRule`
- `rbin:TagResource`
- `rbin:UntagResource`
- `rbin:ListTagsForResource`
- `rbin:LockRule`
- `rbin:UnlockRule`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `tag:GetResources`.

Voici un exemple de politique IAM qui inclut l'autorisation `tag:GetResources` pour les utilisateurs de la console. Si certaines autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "rbin:CreateRule",
      "rbin:UpdateRule",
      "rbin:GetRule",
      "rbin:ListRules",
      "rbin>DeleteRule",
      "rbin:TagResource",
      "rbin:UntagResource",
      "rbin:ListTagsForResource",
      "rbin:LockRule",
```

```
        "rbin:UnlockRule",
        "tag:GetResources"
    ],
    "Resource": "*"
  }]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Autorisations pour utiliser des ressources dans la corbeille

Pour plus d'informations sur les autorisations IAM nécessaires pour travailler avec les ressources de la corbeille, reportez-vous aux rubriques suivantes :

- [Autorisations pour utiliser des instantanés dans la corbeille](#)
- [Autorisations pour utiliser des AMI dans la corbeille](#)

Clés de condition pour la corbeille

La corbeille définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM pour contrôler les conditions d'application de l'instruction de stratégie. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.

Rubriques

- [Clé de condition rbin:Request/ResourceType](#)
- [Clé de condition rbin:Attribute/ResourceType](#)

Clé de condition **rbin:Request/ResourceType**

La clé de rbin:Request/ResourceType condition peut être utilisée pour filtrer l'accès [CreateRule](#) et les [ListRules](#) demandes en fonction de la valeur spécifiée pour le paramètre de ResourceType demande.

Exemple 1 - CreateRule

L'exemple de politique IAM suivant permet aux principaux IAM de faire des CreateRule demandes uniquement si la valeur spécifiée pour le paramètre de ResourceType demande est ou. EBS_SNAPSHOT EC2_IMAGE Cela permet au principal de créer de nouvelles règles de rétention pour les instantanés et les AMI uniquement.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rbin:CreateRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
        }
      }
    }
  ]
}
```

Exemple 2 - ListRules

L'exemple de politique IAM suivant permet aux principaux IAM de faire des ListRules demandes uniquement si la valeur spécifiée pour le paramètre de ResourceType demande est. EBS_SNAPSHOT Cela permet au principal de répertorier les règles de rétention pour les instantanés

uniquement, et cela les empêche de répertorier les règles de rétention pour tout autre type de ressource.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rbin:ListRules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
        }
      }
    }
  ]
}
```

Clé de condition **rbin:Attribute/ResourceType**

La clé de `rbin:Attribute/ResourceType` condition peut être utilisée pour filtrer l'accès sur [DeleteRule](#), [GetRule](#), [UpdateRule](#), [LockRule](#), [UnlockRule](#), [TagResource](#) [UntagResource](#), et les [ListTagsForResource](#) demandes en fonction de la valeur de l'`ResourceType` attribut de la règle de rétention.

Exemple 1 - UpdateRule

L'exemple de politique IAM suivant permet aux principaux IAM de faire des `UpdateRule` demandes uniquement si l'`ResourceType` attribut de la règle de rétention demandée est ou. `EBS_SNAPSHOT` `EC2_IMAGE` Cela permet au principal de mettre à jour des règles de rétention pour les instantanés et les AMI uniquement.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```

        "rbin:UpdateRule"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "rbin:Attribute/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
        }
    }
}
]
}

```

Exemple 2 - DeleteRule

L'exemple de politique IAM suivant permet aux principaux IAM de faire des DeleteRule demandes uniquement si l'ResourceType attribut de la règle de rétention demandée est. EBS_SNAPSHOT Cela permet au principal de supprimer des règles de rétention pour les instantanés uniquement.

```

{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rbin>DeleteRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
        }
      }
    }
  ]
}

```

Utiliser des règles de rétention

Pour activer et utiliser la corbeille, vous devez créer des règles de conservation dans les AWS régions dans lesquelles vous souhaitez protéger vos ressources. Les règles de rétention précisent :

- Le type de ressource que vous souhaitez protéger.

- Les ressources que vous souhaitez retenir dans la corbeille lorsqu'elles sont supprimées.
- La période de rétention pendant laquelle les ressources doivent être retenues dans la corbeille avant d'être définitivement supprimées.

Avec la Corbeille, vous pouvez créer deux types de règles de rétention :

- Règles de rétention au niveau des identifications : une règle de rétention au niveau des identifications utilise des identifications de ressources pour identifier les ressources qui doivent être retenues dans la corbeille. Pour chaque règle de rétention, vous spécifiez une ou plusieurs paires clé-valeur d'identification. Les ressources du type spécifique qui sont étiquetées avec au moins une des paires clé-valeur d'identification qui sont spécifiées dans la règle de rétention sont automatiquement retenues dans la corbeille lors de leur suppression. Utilisez ce type de règle de rétention si vous souhaitez protéger des ressources spécifiques de votre compte en fonction de leurs identifications.
- Règles de rétention au niveau de la Région : aucune identification de ressource n'est spécifiée dans une règle de rétention au niveau de la Région. Elle s'applique à toutes les ressources du type spécifié dans la Région dans laquelle la règle est créée, même si elles ne sont pas étiquetées. Utilisez ce type de règle de rétention si vous souhaitez protéger toutes les ressources d'un type spécifique dans une Région spécifique.

Après avoir créé une règle de rétention, les ressources qui correspondent à ses critères sont automatiquement retenus dans la corbeille pendant la période de rétention spécifiée après leur suppression.

Rubriques

- [Créer une règle de rétention](#)
- [Afficher les règles de rétention de la corbeille](#)
- [Mettre à jour les règles de rétention](#)
- [Verrouillage des règles de conservation](#)
- [Déverrouillage des règles de conservation](#)
- [Étiqueter des règles de rétention](#)
- [Afficher les identifications de règle de rétention](#)
- [Supprimer les identifications des règles de rétention](#)
- [Supprimer des règles de rétention de la corbeille](#)

Créer une règle de rétention

Lorsque vous créez une règle de conservation, vous devez spécifier les paramètres obligatoires suivants :

- Type de ressource devant être protégé par la règle de rétention.
- Types de ressource devant être protégés par la règle de conservation. Vous pouvez créer des règles de conservation au niveau des balises et au niveau de la région.
 - Pour créer une règle de conservation au niveau des balises, spécifiez les balises de ressource qui identifient les ressources à protéger. Vous pouvez spécifier jusqu'à 50 balises pour chaque règle et ajouter la même paire clé-valeur de balise à cinq règles de conservation au maximum.
 - Pour créer une règle de conservation au niveau de la région, ne spécifiez aucune paire clé-valeur de balise. Dans ce cas, toutes les ressources du type spécifié sont protégées.
- La période durant laquelle les ressources sont conservées dans la corbeille après leur suppression. La période peut aller jusqu'à 1 an (365 jours).

Vous pouvez également préciser les paramètres suivants :

- Un nom facultatif pour la règle de rétention. Le nom peut comporter jusqu'à 255 caractères.
- Une description facultative de la règle de rétention. La description peut comporter jusqu'à 255 caractères.

Note

Nous vous recommandons de ne pas inclure de données d'identification personnelle, confidentielles ou sensibles dans la description de la règle de rétention.

- Des identifications de règles de rétention facultatives pour faciliter l'identification et l'organisation de vos règles de rétention. Vous pouvez attribuer jusqu'à 50 identifications à chaque règle.

Vous pouvez également verrouiller les règles de conservation lors de la création. Si vous verrouillez une règle de conservation lors de sa création, vous devez également spécifier le délai de déverrouillage, qui peut aller de 7 à 30 jours. Les règles de conservation restent déverrouillées par défaut, à moins que vous ne les verrouilliez explicitement.

Les règles de rétention fonctionnent uniquement dans les régions où elles ont été créées. Si vous avez l'intention d'utiliser la corbeille dans d'autres régions, vous devez créer des règles de rétention supplémentaires dans ces régions.

Vous pouvez créer une règle de rétention de corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour créer une règle de rétention

1. Ouvrez la console de corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>.
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention), puis Create retention rule (Créer une règle de rétention).
3. Dans la section Rule details (Détails de la règle), procédez comme suit :
 - a. (Facultatif) Pour Retention rule name (Nom de la règle de rétention), saisissez un nom descriptif pour la règle de rétention.
 - b. (Facultatif) Pour Retention rule description (Description de la règle de rétention), saisissez une brève description pour la règle de rétention.
4. Dans la section Rule settings (Paramètres de la règle), procédez comme suit :
 - a. Pour Resource type (Type de ressource), sélectionnez le type de ressource devant être protégé par la règle de rétention. La règle de rétention conservera uniquement les ressources de ce type dans la corbeille.
 - b. Effectuez l'une des actions suivantes :
 - Pour créer une règle de rétention de niveau Région qui correspond à toutes les ressources d'un type spécifié supprimées de la Région, sélectionnez Apply to all resources (Appliquer à l'ensemble des ressources). La règle de rétention retiendra toutes les ressources supprimées du type spécifié dans la corbeille lors de la suppression, même si les ressources ne comportent aucune identification.
 - Pour créer une règle de rétention de niveau identification, pour Resource tags to match (Identifications de ressources à faire correspondre), saisissez les paires clé-valeur d'identifications à utiliser pour identifier les ressources du type spécifié qui doivent être retenues dans la corbeille. Seules les ressources du type spécifié qui ont au moins une des paires clé-valeur spécifiées seront retenues par la règle de rétention.
 - c. Pour Retention period (Période de rétention), saisissez le nombre de jours pendant lesquels la règle de rétention doit retenir les ressources dans la corbeille.

5. (Facultatif) Pour verrouiller la règle de conservation, dans Rule lock settings (Paramètres de verrouillage des règles), sélectionnez Lock (Verrouiller), puis dans Unlock delay period (Délai de déverrouillage), spécifiez le délai de déverrouillage en jours. Une règle de conservation verrouillée ne peut être ni modifiée ni supprimée. Pour modifier ou supprimer la règle, vous devez d'abord la déverrouiller, puis attendre l'expiration du délai de déverrouillage. Pour plus d'informations, consultez [Verrouillage des règles de conservation](#).

Pour laisser la règle de conservation déverrouillée, dans Rule lock settings (Paramètres de verrouillage des règles), conservez l'option Unlock (Déverrouiller). Une règle de conservation déverrouillée peut être modifiée ou supprimée à tout moment. Pour plus d'informations, consultez [Déverrouillage des règles de conservation](#).

6. (Facultatif) Dans la section Tags (Identifications), procédez comme suit :
 - Pour étiqueter la règle avec des identifications personnalisées, choisissez Add tag (Ajouter une identification) puis saisissez la paire clé-valeur d'identification.
7. Choisissez Create retention rule (Créer une règle de rétention).

AWS CLI

Pour créer une règle de rétention

Utilisez la commande [create-rule](#) de la AWS CLI . Pour `--retention-period`, spécifiez le nombre de jours de rétention des instantanés supprimés dans la corbeille. Pour `--resource-type`, spécifiez `EBS_SNAPSHOT` pour les instantanés ou `EC2_IMAGE` pour les AMI. Pour créer une règle de rétention au niveau des identifications, pour `--resource-tags`, spécifiez les identifications à utiliser afin d'identifier les instantanés à retenir. Pour créer une règle de conservation au niveau de la région, omettez `--resource-tags`. Pour verrouiller une règle de conservation, incluez `--lock-configuration` et spécifiez le délai de déverrouillage en jours.

```
aws rbin create-rule \  
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT|EC2_IMAGE \  
--description "rule_description" \  
--lock-configuration  
'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \  
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

Exemple 1

L'exemple de commande suivant crée une règle de conservation au niveau de la région déverrouillée qui conserve tous les instantanés supprimés pendant une période de 7 jours.

```
aws rbin create-rule \  
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT \  
--description "Match all snapshots"
```

Exemple 2

L'exemple de commande suivant crée une règle de niveau identification qui retient les instantanés supprimés qui sont étiquetés `purpose=production` pendant une période de 7 jours.

```
aws rbin create-rule \  
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT \  
--description "Match snapshots with a specific tag" \  
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

Exemple 3

L'exemple de commande suivant crée une règle de conservation au niveau de la région verrouillée qui conserve tous les instantanés supprimés pendant une période de 7 jours. La règle de conservation est verrouillée avec un délai de déverrouillage de 7 jours.

```
aws rbin create-rule \  
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT \  
--description "Match all snapshots" \  
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

Afficher les règles de rétention de la corbeille

Vous pouvez créer une règle de rétention de la corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour afficher les règles de rétention

1. Ouvrez la console de corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>.

2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. La grille liste toutes les règles de rétention de la région sélectionnée. Pour afficher des informations supplémentaires sur une règle de rétention spécifique, sélectionnez-la dans la grille.

AWS CLI

Pour afficher toutes vos règles de rétention

Utilisez la commande d' AWS CLI [list-rules](#), et pour `--resource-type`, spécifiez `EBS_SNAPSHOT` pour les instantanés ou `EC2_IMAGE` pour les AMI.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT|EC2_IMAGE
```

Exemple

L'exemple de commande suivant répertorie toutes les règles de rétention qui retiennent les instantanés.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT
```

Pour afficher les informations relatives à une règle de rétention spécifique

Utilisez la commande [get-rule](#) AWS CLI .

```
aws rbin get-rule --identifiant rule_ID
```

Exemple

L'exemple de commande suivant fournit des informations sur la règle de rétention `pwxIkFcvge4`.

```
aws rbin get-rule --identifiant pwxIkFcvge4
```

Mettre à jour les règles de rétention

Vous pouvez mettre à jour la description d'une règle de conservation déverrouillée, ses balises de ressource et sa période de conservation à tout moment après sa création. Vous ne pouvez pas mettre à jour le type de ressource ou le délai de déverrouillage d'une règle de conservation, même si la règle de conservation est déverrouillée.

Vous ne pouvez en aucun cas mettre à jour une règle de conservation verrouillée. Si vous devez modifier une règle de conservation verrouillée, vous devez d'abord la déverrouiller, puis attendre l'expiration du délai de déverrouillage.

Si vous devez modifier le délai de déverrouillage d'une règle de conservation verrouillée, vous devez [déverrouiller la règle de conservation](#), puis attendre l'expiration du délai de déverrouillage actuel. Lorsque le délai de déverrouillage est expiré, vous devez [verrouiller à nouveau la règle de conservation](#) et spécifier le nouveau délai de déverrouillage.

Note

Nous vous recommandons de ne pas inclure de données d'identification personnelle, confidentielles ou sensibles dans la description de la règle de rétention.

Une fois que vous avez mis à jour une règle de rétention, les modifications s'appliquent uniquement aux nouvelles ressources qu'elle retient. Les modifications n'affectent pas les ressources précédemment envoyées à la corbeille. Par exemple, si vous mettez à jour la période de rétention d'une règle de rétention, seuls les instantanés supprimés après la mise à jour sont retenus pour la nouvelle période de rétention. Les instantanés envoyés à la corbeille avant la mise à jour sont retenus pendant la période de rétention précédente (ancienne).

Vous pouvez mettre à jour une règle de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour mettre à jour une règle de rétention

1. Ouvrez la console de corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>.
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de rétention à mettre à jour, puis choisissez Actions, Edit retention rule (Modifier une règle de rétention).
4. Dans la section Rule details (Détails de la règle), mettez à jour Retention rule name (Nom de la règle de rétention) et Retention rule description (Description de la règle de rétention), si nécessaire.
5. Dans la section Rule settings (Paramètres de la règle), mettez à jour Resource type (Type de ressource), Resource tags to match (Identifications de ressource à faire correspondre) et Retention period (Période de rétention), si nécessaire.

6. Dans la section Tags (Identifications), ajoutez ou supprimez des identifications de règles de rétention si nécessaire.
7. Choisissez Save retention rule (Enregistrer la règle de rétention).

AWS CLI

Pour mettre à jour une règle de rétention

Utilisez la commande [update-site](#) de la AWS CLI . Pour `--identifier`, spécifiez l'ID de la règle de rétention à mettre à jour. Pour `--resource-types`, spécifiez `EBS_SNAPSHOT` pour les instantanés ou `EC2_IMAGE` pour les AMI.

```
aws rbin update-rule \  
--identifier rule_ID \  
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT|EC2_IMAGE \  
--description "rule_description"
```

Exemple

L'exemple de commande suivant met à jour la règle de rétention `61sJ2Fa9nh9` pour retenir tous les instantanés pour 7 jours et met à jour sa description.

```
aws rbin update-rule \  
--identifier 61sJ2Fa9nh9 \  
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT \  
--description "Retain for three weeks"
```

Verrouillage des règles de conservation

La corbeille vous permet de verrouiller les règles de conservation au niveau de la région à tout moment.

Note

Vous ne pouvez pas verrouiller les règles de conservation au niveau des balises.

Une règle de conservation verrouillée ne peut être ni modifiée ni supprimée, même par les utilisateurs disposant des autorisations IAM requises. Verrouillez vos règles de conservation pour les protéger contre les modifications et les suppressions accidentelles ou malveillantes.

Lorsque vous verrouillez une règle de conservation, vous devez spécifier un délai de déverrouillage. Il s'agit de la période de temps que vous devez attendre après avoir déverrouillé la règle de conservation avant de pouvoir la modifier ou la supprimer. Vous ne pouvez ni modifier ni supprimer la règle de conservation pendant le délai de déverrouillage. Vous pouvez modifier ou supprimer la règle de conservation qu'une fois le délai de déverrouillage expiré.

Vous ne pouvez pas modifier la période de déverrouillage après le verrouillage de la règle de conservation. Si les autorisations de votre compte ont été compromises, le délai de déverrouillage vous donne plus de temps pour détecter les menaces de sécurité et y répondre. La durée de cette période doit être plus longue que le temps nécessaire à pour identifier les failles de sécurité et y répondre. Pour définir la durée appropriée, vous pouvez passer en revue les incidents de sécurité précédents et le temps nécessaire pour identifier et corriger une violation de compte.

Nous vous recommandons d'utiliser EventBridge les règles Amazon pour vous informer des modifications de l'état de verrouillage des règles de rétention. Pour plus d'informations, consultez [Surveillez la corbeille à l'aide d'Amazon EventBridge](#).

Considérations

- Vous pouvez verrouiller les règles de conservation au niveau de la région uniquement.
- Vous pouvez verrouiller une règle de conservation déverrouillée à tout moment.
- Le délai de déverrouillage doit être de 7 à 30 jours.
- Vous pouvez verrouiller à nouveau une règle de conservation pendant le délai de déverrouillage. Verrouiller à nouveau la règle de conservation réinitialise le délai de déverrouillage.

Vous pouvez verrouiller une règle de conservation au niveau de la région à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour verrouiller une règle de conservation

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le panneau de navigation, choisissez Retention rules (Règles de rétention).

3. Dans la grille, sélectionnez la règle de conservation déverrouillée que vous souhaitez verrouiller, puis choisissez Actions, Edit retention rule lock (Modifier le verrouillage d'une règle de conservation).
4. Dans l'écran Edit retention rule lock (Modifier le verrouillage d'une règle de conservation), choisissez Lock (Verrouiller), puis pour Unlock delay period (Délai de déverrouillage), spécifiez le délai de déverrouillage en jours.
5. Cochez la case I acknowledge that locking the retention rule will prevent it from being modified or deleted (Je reconnais que le verrouillage de la règle de conservation empêchera sa modification ou sa suppression), puis choisissez Save (Enregistrer).

AWS CLI

Pour verrouiller une règle de conservation déverrouillée

Utilisez la commande AWS CLI [lock-rule](#). Pour `--identifiant`, spécifiez l'ID de la règle de conservation à verrouiller. Pour `--lock-configuration`, spécifiez le délai de déverrouillage en jours.

```
aws rbin lock-rule \  
--identifiant rule_ID \  
--lock-configuration  
'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

Exemple

L'exemple de commande suivant verrouille la règle de conservation 61sJ2Fa9nh9 et définit le délai de déverrouillage sur 15 jours.

```
aws rbin lock-rule \  
--identifiant 61sJ2Fa9nh9 \  
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

Déverrouillage des règles de conservation

Vous ne pouvez ni modifier ni supprimer une règle de conservation verrouillée. Si vous devez modifier une règle de conservation verrouillée, vous devez d'abord la déverrouiller. Après avoir déverrouillé la règle de conservation, vous devez attendre l'expiration du délai de déverrouillage

avant de la modifier ou de la supprimer. Vous ne pouvez ni modifier ni supprimer une règle de conservation pendant le délai de déverrouillage.

Une règle de conservation déverrouillée peut être modifiée et supprimée à tout moment par un utilisateur disposant des autorisations IAM requises. Le fait de laisser vos règles de conservation déverrouillées peut les exposer à des modifications et à des suppressions accidentelles ou malveillantes.

Considérations

- Vous pouvez verrouiller à nouveau une règle de conservation pendant le délai de déverrouillage.
- Vous pouvez verrouiller à nouveau une règle de conservation une fois le délai de déverrouillage expiré.
- Vous ne pouvez pas contourner le délai de déverrouillage.
- Vous ne pouvez pas modifier le délai de déverrouillage après le verrouillage initial.

Nous vous recommandons d'utiliser EventBridge les règles Amazon pour vous informer des modifications de l'état de verrouillage des règles de rétention. Pour plus d'informations, consultez [Surveillez la corbeille à l'aide d'Amazon EventBridge](#).

Vous pouvez déverrouiller une règle de conservation au niveau de la région à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour déverrouiller une règle de conservation

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le panneau de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de conservation verrouillée que vous souhaitez déverrouiller, puis choisissez Actions, Edit retention rule lock (Modifier le verrouillage d'une règle de conservation).
4. Sur l'écran Edit retention rule lock (Modifier le verrouillage d'une règle de conservation), choisissez Unlock (Déverrouiller), puis Save (Enregistrer).

AWS CLI

Pour déverrouiller une règle de conservation verrouillée

Utilisez la commande AWS CLI [unlock-rule](#). Pour `--identifieur`, spécifiez l'ID de la règle de conservation à déverrouiller.

```
aws rbin unlock-rule \  
--identifieur rule_ID
```

Exemple

L'exemple de commande suivant déverrouille la règle de conservation 61sJ2Fa9nh9

```
aws rbin unlock-rule \  
--identifieur 61sJ2Fa9nh9
```

Étiqueter des règles de rétention

Vous pouvez affecter des identifications personnalisées à vos règles de rétention pour classer celles-ci de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Cela vous permet de trouver de manière efficace une règle de rétention spécifique en fonction des identifications personnalisées que vous avez affectées.

Vous pouvez affecter une identification à une règle de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour étiqueter une règle de rétention

1. Ouvrez la console de corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>.
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Sélectionnez la règle de rétention à étiqueter, choisissez l'onglet Tags (Identifications), puis choisissez Manage tags (Gérer les identifications).
4. Choisissez Ajouter une balise. Pour Key (Clé), saisissez la clé de l'identification. Pour Value (Valeur), saisissez la valeur de l'identification.
5. Choisissez Save (Enregistrer).

AWS CLI

Pour étiqueter une règle de rétention

Utilisez la commande [tag-resource](#) AWS CLI . Pour `--resource-arn`, indiquez l'Amazon Resource Name (ARN) de la règle de rétention à étiqueter, et pour `--tags`, spécifiez la paire clé-valeur d'identification.

```
aws rbin tag-resource \  
--resource-arn retention_rule_arn \  
--tags key=tag_key,value=tag_value
```

Exemple

L'exemple de commande suivant étiquette la règle de rétention `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3` avec l'identification `purpose=production`.

```
aws rbin tag-resource \  
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3 \  
--tags key=purpose,value=production
```

Afficher les identifications de règle de rétention

Vous pouvez afficher les identifications affectées à une règle de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour afficher les identifications d'une règle de rétention

1. Ouvrez la console de corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>.
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Sélectionnez la règle de rétention pour laquelle afficher les identifications, puis choisissez l'onglet Tags (Identifications).

AWS CLI

Pour afficher les identifications affectées à une règle de rétention

Utilisez la commande [list-tags-for-resource](#) de la AWS CLI . Pour `--resource-arn`, spécifiez l'ARN de la règle de rétention.

```
aws rbin list-tags-for-resource \  

```

```
--resource-arn retention_rule_arn
```

Exemple

L'exemple de commande suivant répertorie les identifications de règle de rétention `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3`.

```
aws rbin list-tags-for-resource \  
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3
```

Supprimer les identifications des règles de rétention

Vous pouvez supprimer les identifications d'une règle de rétention en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour supprimer une identification d'une règle de rétention

1. Ouvrez la console de corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>.
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Sélectionnez la règle de rétention dont vous souhaitez supprimer une identification et choisissez Tags (Identifications), puis Manage tags (Gérer les identifications).
4. Choisissez Remove (Supprimer) en regard de l'identification à supprimer.
5. Choisissez Save (Enregistrer).

AWS CLI

Pour supprimer une identification d'une règle de rétention

Utilisez la commande [untag-resource](#) de la AWS CLI . Pour `--resource-arn`, spécifiez l'ARN de la règle de rétention. Pour `--tagkeys`, spécifiez les clés d'identifications des identifications à supprimer.

```
aws rbin untag-resource \  
--resource-arn retention_rule_arn \  
--tagkeys tag_key
```

Exemple

Voici un exemple de commande supprimant les identifications disposant d'une clé d'identification de type `purpose` de la règle de rétention `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3`.

```
aws rbin untag-resource \  
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3 \  
--tagkeys purpose
```

Supprimer des règles de rétention de la corbeille

Vous pouvez supprimer une règle de rétention à tout moment. Lorsque vous supprimez une règle de rétention, elle ne retient plus les nouvelles ressources dans la corbeille une fois qu'elles ont été supprimées. Les ressources envoyées à la corbeille avant la suppression de la règle de rétention continuent d'être retenues dans la corbeille en fonction de la période de rétention définie dans la règle de rétention. Lorsque la période expire, l'instantané est définitivement supprimé de la corbeille.

Vous pouvez supprimer une règle de rétention en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour supprimer une règle de rétention

1. Ouvrez la console de corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>.
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de rétention à supprimer, puis choisissez Actions, Delete retention rule (Supprimer la règle de rétention).
4. Lorsque vous y êtes invité, saisissez le message de confirmation et choisissez Delete retention rule (Supprimer la règle de rétention).

AWS CLI

Pour supprimer une règle de rétention

Utilisez la commande [delete-rule](#) de la AWS CLI . Pour `--identifier`, spécifiez l'ID de la règle de rétention à supprimer.

```
aws rbin delete-rule --identifiant rule_ID
```

Exemple

L'exemple de commande suivant supprime la règle de rétention 61sJ2Fa9nh9.

```
aws rbin delete-rule --identifiant 61sJ2Fa9nh9
```

Utiliser des ressources dans la corbeille

La corbeille prend en charge les types de ressources suivants :

- Instantanés Amazon EBS
- Amazon Machine Images (AMI) basées sur Amazon EBS

Tâches

- [Récupérer des instantanés à partir de la corbeille](#)
- [Récupérer des instantanés depuis la corbeille](#)

Récupérer des instantanés à partir de la corbeille

La corbeille est une fonction de récupération de données qui vous permet de restaurer des instantanés Amazon EBS et des AMI basées sur EBS supprimés accidentellement. Lorsque vous utilisez la corbeille, si vos ressources sont supprimées, elles sont retenues dans la corbeille pendant une période spécifiée avant leur suppression définitive.

Vous pouvez restaurer une ressource à partir de la corbeille à tout moment avant l'expiration de sa période de rétention. Une fois que vous avez restauré une ressource à partir de la corbeille, elle est supprimée de la corbeille et vous pouvez l'utiliser de la même manière que n'importe quelle autre ressource de ce type sur votre compte. Si la période de rétention expire et que la ressource n'est pas restaurée, elle est définitivement supprimée de la corbeille et n'est plus disponible pour restauration.

Les instantanés dans la corbeille sont facturés au même tarif que les instantanés courants de votre compte. Il n'y a pas de facturation supplémentaire pour l'utilisation de la corbeille et des règles de rétention. Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

Pour plus d'informations, consultez [Corbeille](#).

Rubriques

- [Autorisations pour utiliser des instantanés dans la corbeille](#)
- [Afficher les instantanés dans la corbeille](#)
- [Restaurer des instantanés à partir de la corbeille](#)

Autorisations pour utiliser des instantanés dans la corbeille

Par défaut, les utilisateurs ne sont pas autorisés à utiliser les instantanés contenus dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Pour afficher et récupérer des instantanés qui se trouvent dans la corbeille, les utilisateurs doivent disposer des autorisations suivantes :

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Pour gérer les identifications des instantanés dans la corbeille, les utilisateurs ont besoin des autorisations supplémentaires suivantes.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `ec2:DescribeTags`.

Voici un exemple de politique IAM. Elle comprend l'autorisation `ec2:DescribeTags` pour les utilisateurs de la console et les autorisations `ec2:CreateTags` et `ec2:DeleteTags` pour la gestion des identifications. Si les autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:ListSnapshotsInRecycleBin",
    "ec2:RestoreSnapshotFromRecycleBin"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:DescribeTags"
  ],
  "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
},
]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations nécessaires pour utiliser la corbeille, consultez [Autorisations pour utiliser la corbeille et les règles de rétention](#).

Afficher les instantanés dans la corbeille

Lorsqu'un instantané se trouve dans la corbeille, vous pouvez afficher des informations limitées à son sujet, notamment :

- ID de l'instantané
- la description de l'instantané ;
- l'ID du volume à partir duquel l'instantané a été créé ;
- la date et l'heure de la suppression de l'instantané et de son entrée dans la corbeille ;
- la date et l'heure d'expiration de la période de rétention ; à ce moment-là, l'instantané sera définitivement supprimé de la corbeille.

Vous pouvez afficher les instantanés dans la corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour visualiser les instantanés dans la corbeille à l'aide de la console

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie tous les instantanés qui se trouvent actuellement dans la corbeille. Pour afficher les détails d'un instantané spécifique, sélectionnez-le dans la grille et choisissez Actions, View details (Afficher les détails).

AWS CLI

Pour afficher des instantanés dans la corbeille à l'aide du AWS CLI

Utilisez la commande [AWS CLI list-snapshots-in-recycle-bin](#). Incluez l'option `--snapshot-id` pour afficher un instantané spécifique ou omettez l'option `--snapshot-id` pour afficher tous les instantanés dans la corbeille.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Par exemple, la commande suivante renvoie des informations sur l'instantané `snap-01234567890abcdef` dans la corbeille.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Exemple de sortie :

```
{
  "SnapshotRecycleBinInfo": [
    {
      "Description": "Monthly data backup snapshot",
      "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
      "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
      "VolumeId": "vol-abcdef09876543210",
      "SnapshotId": "snap-01234567890abcdef"
    }
  ]
}
```

Restaurer des instantanés à partir de la corbeille

Vous ne pouvez en aucun cas utiliser un instantané lorsqu'il se trouve dans la corbeille. Pour utiliser l'instantané, vous devez d'abord le restaurer. Lorsque vous restaurez un instantané à partir de la corbeille, il est immédiatement disponible pour utilisation et il est supprimé de la corbeille. Une fois qu'il est restauré, vous pouvez l'utiliser de la même manière que n'importe quel autre instantané de votre compte.

Vous pouvez restaurer un instantané à partir de la corbeille en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour restaurer un instantané à partir de la corbeille en utilisant la console

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie tous les instantanés qui se trouvent actuellement dans la corbeille. Sélectionnez l'instantané à restaurer, puis choisissez Recover (Récupérer).
4. Lorsque vous y êtes invité, choisissez Recover (Récupérer).

AWS CLI

Pour restaurer un instantané supprimé de la corbeille à l'aide du AWS CLI

Utilisez la commande [restore-snapshot-from-recycle-bin](#) AWS CLI . Pour `--snapshot-id`, spécifiez l'ID de l'instantané à restaurer.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Par exemple, la commande suivante restaure l'instantané `snap-01234567890abcdef` depuis la corbeille.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

Exemple de sortie :

```
{
  "SnapshotId": "snap-01234567890abcdef",
  "Description": "Monthly data backup snapshot",
  "Encrypted": false,
  "OwnerId": "111122223333",
  "Progress": "100%",
  "StartTime": "2021-12-01T13:00:00.000000+00:00",
  "State": "recovering",
  "VolumeId": "vol-ffffffff",
  "VolumeSize": 30
}
```

Récupérer des instantanés depuis la corbeille

La corbeille est une fonction de récupération de données qui vous permet de restaurer des instantanés Amazon EBS et des AMI basées sur EBS supprimés accidentellement. Lorsque vous utilisez la corbeille, si vos ressources sont supprimées, elles sont retenues dans la corbeille pendant une période spécifiée avant leur suppression définitive.

Vous pouvez restaurer une ressource à partir de la corbeille à tout moment avant l'expiration de sa période de rétention. Une fois que vous avez restauré une ressource à partir de la corbeille, elle est supprimée de la corbeille et vous pouvez l'utiliser de la même manière que n'importe quelle autre ressource de ce type sur votre compte. Si la période de rétention expire et que la ressource n'est pas restaurée, elle est définitivement supprimée de la corbeille et n'est plus disponible pour restauration.

Les AMI de la corbeille n'entraînent pas de frais supplémentaires.

Pour plus d'informations, consultez [Corbeille](#).

Rubriques

- [Autorisations pour utiliser des AMI dans la corbeille](#)
- [Afficher les AMI dans la corbeille](#)
- [Restaurer des AMI depuis la corbeille](#)

Autorisations pour utiliser des AMI dans la corbeille

Par défaut, les utilisateurs ne sont pas autorisés à utiliser les AMI contenues dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Pour afficher et récupérer des AMI qui se trouvent dans la corbeille, les utilisateurs doivent disposer des autorisations suivantes :

- `ec2:ListImagesInRecycleBin`
- `ec2:RestoreImageFromRecycleBin`

Pour gérer les identifications des AMI dans la corbeille, les utilisateurs ont besoin des autorisations supplémentaires suivantes.

- `ec2:CreateTags`
- `ec2>DeleteTags`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `ec2:DescribeTags`.

Voici un exemple de politique IAM. Elle comprend l'autorisation `ec2:DescribeTags` pour les utilisateurs de la console et les autorisations `ec2:CreateTags` et `ec2>DeleteTags` pour la gestion des identifications. Si les autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:ListImagesInRecycleBin",
    "ec2:RestoreImageFromRecycleBin"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:DescribeTags"
  ],
  "Resource": "arn:aws:ec2:Region::image/*"
}
]
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) du Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations nécessaires pour utiliser la corbeille, consultez [Autorisations pour utiliser la corbeille et les règles de rétention](#).

Afficher les AMI dans la corbeille

Lorsqu'une AMI se trouve dans la corbeille, vous pouvez afficher des informations limitées à son sujet, notamment :

- Le nom, la description et l'ID unique de l'AMI.
- La date et l'heure de la suppression de l'AMI et de son entrée dans la corbeille.
- la date et l'heure d'expiration de la période de rétention ; L'AMI sera définitivement supprimée à ce moment-là.

Vous pouvez afficher les AMI dans la corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour visualiser les AMI supprimées dans la corbeille à l'aide de la console

1. Ouvrez la console de la corbeille à l'adresse console.aws.amazon.com/rbin/home/.
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie toutes les ressources qui se trouvent actuellement dans la corbeille. Pour afficher les détails d'une AMI spécifique, sélectionnez-la dans la grille et choisissez Actions, View details (Afficher les détails).

AWS CLI

Pour afficher les AMI supprimées dans la corbeille à l'aide du AWS CLI

Utilisez la AWS CLI commande [list-images-in-recycle-bin](#). Pour afficher des AMI spécifiques, incluez l'option `--image-id` et spécifiez les ID des AMI à afficher. Vous pouvez spécifier jusqu'à 20 ID dans une seule demande.

Pour afficher toutes les AMI de la corbeille, omettez l'option `--image-id`. Si vous ne spécifiez pas de valeur pour `--max-items`, la commande renvoie par défaut 1 000 éléments par page. Pour plus d'informations, consultez [Pagination](#) dans le manuel Amazon EC2 API Reference.

```
aws ec2 list-images-in-recycle-bin --image-id ami_id
```

Par exemple, la commande suivante renvoie des informations sur l'AMI `ami-01234567890abcdef` dans la corbeille.

```
aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

Exemple de sortie :

```
{
  "Images": [
    {
      "ImageId": "ami-0f740206c743d75df",
      "Name": "My AL2 AMI",
      "Description": "My Amazon Linux 2 AMI",
      "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
      "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
    }
  ]
}
```

Important

Si le message d'erreur suivant s'affiche, il se peut que vous deviez mettre à jour votre AWS CLI version. Pour plus d'informations, veuillez consulter la rubrique [Erreurs liées aux commandes introuvables](#).

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

Restaurer des AMI depuis la corbeille

Vous ne pouvez en aucun cas utiliser une AMI lorsqu'elle se trouve dans la corbeille. Pour utiliser l'AMI, vous devez d'abord la restaurer. Lorsque vous restaurez une AMI à partir de la corbeille, elle est immédiatement disponible pour utilisation et elle est supprimée de la corbeille. Une fois qu'elle est restaurée, vous pouvez l'utiliser de la même manière que n'importe quelle autre AMI de votre compte.

Vous pouvez restaurer une AMI à partir de la corbeille en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour restaurer une AMI depuis la corbeille en utilisant la console

1. Ouvrez la console de la corbeille à l'adresse console.aws.amazon.com/rbin/home/.

2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie toutes les ressources qui se trouvent actuellement dans la corbeille. Sélectionnez l'AMI à restaurer, puis choisissez Recover (Récupérer).
4. Lorsque vous y êtes invité, choisissez Recover (Récupérer).

AWS CLI

Pour restaurer une AMI supprimée de la corbeille à l'aide du AWS CLI

Utilisez la AWS CLI commande [restore-image-from-recycle-bin](#). Pour `--image-id`, spécifiez l'ID de l'AMI à restaurer.

```
aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

Par exemple, la commande suivante restaure l'AMI `ami-01234567890abcdef` depuis la corbeille.

```
aws ec2 restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

La commande ne renvoie aucun résultat en cas de succès.

Important

Si le message d'erreur suivant s'affiche, il se peut que vous deviez mettre à jour votre AWS CLI version. Pour plus d'informations, veuillez consulter la rubrique [Erreurs liées aux commandes introuvables](#).

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

Surveiller la corbeille

Vous pouvez utiliser les fonctions suivantes pour surveiller la corbeille.

Rubriques

- [Surveillez la corbeille à l'aide d'Amazon EventBridge](#)

- [Surveillez l'utilisation de la corbeille AWS CloudTrail](#)

Surveillez la corbeille à l'aide d'Amazon EventBridge

La corbeille envoie des événements à Amazon EventBridge pour les actions effectuées sur les règles de rétention. Avec EventBridge, vous pouvez établir des règles qui initient des actions programmatiques en réponse à ces événements. Par exemple, vous pouvez créer une EventBridge règle qui envoie une notification à votre adresse e-mail lorsqu'une règle de rétention est déverrouillée et qu'elle entre dans son délai de déverrouillage. Pour plus d'informations, consultez [la section Création de EventBridge règles Amazon qui réagissent aux événements](#).

Les événements dans EventBridge sont représentés sous forme d'objets JSON. Les champs spécifiques à l'événement figurent dans la section `detail` de l'objet JSON. Le champ `event` contient le nom de l'événement. Le champ `result` contient l'état terminé de l'action qui lance l'événement. Pour plus d'informations, consultez les [modèles EventBridge d'événements Amazon](#) dans le guide de EventBridge l'utilisateur Amazon.

Pour plus d'informations sur Amazon EventBridge, consultez [Qu'est-ce qu'Amazon EventBridge ?](#) dans le guide de EventBridge l'utilisateur Amazon.

Événements

- [RuleLocked](#)
- [RuleChangeTentative](#)
- [RuleUnlockProgrammé](#)
- [RuleUnlockingAvis](#)
- [RuleUnlocked](#)

RuleLocked

Voici un exemple d'événement généré par la corbeille lorsqu'une règle de conservation est correctement verrouillée. Cet événement peut être généré par `CreateRule` ou `LockRule`. L'API qui a généré l'événement est indiquée dans le champ `api-name`.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Locked",
```

```
"source": "aws.rbin",
"account": "123456789012",
"time": "2022-08-10T16:37:50Z",
"region": "us-west-2",
"resources": [
  "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
],
"detail": {
  "detail-version": " 1.0.0",
  "rule-id": "a12345abcde",
  "rule-description": "locked account level rule",
  "unlock-delay-period": "30 days",
  "api-name": "CreateRule"
}
}
```

RuleChangeTentative

Voici un exemple d'événement généré par la corbeille lors de tentatives infructueuses de modification ou de suppression d'une règle verrouillée. Cet événement peut être généré par `DeleteRule` ou `UpdateRule` demandés. L'API qui a généré l'événement est indiquée dans le champ `api-name`.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Change Attempted",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail": {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "DeleteRule"
  }
}
```

RuleUnlockProgrammé

Voici un exemple d'événement généré par la corbeille lorsqu'une règle de conservation est déverrouillée et qu'elle commence son délai de déverrouillage.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlock Scheduled",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail": {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z",
  }
}
```

RuleUnlockingAvis

Voici un exemple d'événement généré quotidiennement par la corbeille alors qu'une règle de conservation est dans son délai de déverrouillage, jusqu'à la veille de l'expiration du délai de déverrouillage.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocking Notice",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
}
```

```
"detail":
{
  "detail-version": " 1.0.0",
  "rule-id": "a12345abcde",
  "rule-description": "locked account level rule",
  "unlock-delay-period": "30 days",
  "scheduled-unlock-time": "2022-09-10T16:37:50Z"
}
}
```

RuleUnlocked

Voici un exemple d'événement généré par la corbeille lorsque le délai de déverrouillage d'une règle de conservation expire et que la règle de rétention peut être modifiée ou supprimée.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

Surveillez l'utilisation de la corbeille AWS CloudTrail

Le service Recycle Bin est intégré à AWS CloudTrail. CloudTrail est un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture tous les appels d'API effectués dans la corbeille sous forme d'événements. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un bucket Amazon

Simple Storage Service (Amazon S3). Si vous ne configurez pas de suivi, vous pouvez toujours consulter les derniers événements de gestion dans la CloudTrail console dans Historique des événements. Vous pouvez utiliser les informations collectées CloudTrail pour déterminer la demande qui a été faite à Recycle Bin, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des informations supplémentaires.

Pour plus d'informations CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Informations sur la corbeille dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité événementielle prise en charge se produit dans la corbeille, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte.

Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements de votre AWS compte, y compris les événements liés à Recycle Bin, créez un parcours. Un journal permet CloudTrail de fournir des fichiers journaux à un compartiment S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez la section [Overview for creating a trail](#) dans le Guide de l'utilisateur AWS CloudTrail .

Actions d'API prises en charge

Pour Recycle Bin, vous pouvez CloudTrail enregistrer les actions d'API suivantes en tant qu'événements de gestion.

- CreateRule
- UpdateRule
- GetRules
- ListRule
- DeleteRule
- TagResource
- UntagResource

- ListTagsForResource
- LockRule
- UnlockRule

Pour plus d'informations sur les événements de gestion de journalisation, consultez la section [Événements de gestion de journalisation pour les sentiers](#) dans le guide de CloudTrail l'utilisateur.

Informations relatives à l'identité

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'[CloudTrail utilisateur IdentityElement](#).

Comprendre les entrées du fichier journal de la corbeille

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Voici des exemples d'entrées de CloudTrail journal.

CreateRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
```

```
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
},
"webIdFederationData": {},
"attributes": {
  "mfaAuthenticated": "false",
  "creationDate": "2021-08-02T21:43:38Z"
}
},
"eventTime": "2021-08-02T21:45:22Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "CreateRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
  "retentionPeriod": {
    "retentionPeriodValue": 7,
    "retentionPeriodUnit": "DAYS"
  },
  "description": "Match all snapshots",
  "resourceType": "EBS_SNAPSHOT"
},
"responseElements": {
  "identifier": "jkrnexample"
},
"requestID": "ex0577a5-amc4-pl14f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
```

```

    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}

```

GetRule

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:33Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "GetRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 boto3/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",

```

```

"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

ListRules

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:44:37Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListRules",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",

```

```

"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 boto-core/1.21.9",
"requestParameters": {
  "resourceTags": [
    {
      "resourceTagKey": "test",
      "resourceTagValue": "test"
    }
  ]
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

UpdateRule

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      }
    }
  },

```

```

    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-08-02T21:43:38Z"
    }
  },
  "eventTime": "2021-08-02T21:46:03Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UpdateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 boto3/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample",
    "retentionPeriod": {
      "retentionPeriodValue": 365,
      "retentionPeriodUnit": "DAYS"
    }
  },
  "description": "Match all snapshots",
  "resourceType": "EBS_SNAPSHOT"
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

DeleteRule

```

{
  "eventVersion": "1.08",
  "userIdentity": {

```

```
"type": "AssumedRole",
"principalId": "123456789012",
"arn": "arn:aws:iam::123456789012:root",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
}
},
"eventTime": "2021-08-02T21:46:25Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "DeleteRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 boto-core/1.21.9",
"requestParameters": {
  "identifier": "jkrnexample"
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```

```
}
```

TagResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    },
  },
  "eventTime": "2021-10-22T21:43:15Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "TagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 boto3/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tags": [
      {
        "key": "purpose",
        "value": "production"
      }
    ]
  }
},
```

```

"responseElements": null,
"requestID": "examplee-7962-49ec-8633-795efexample",
"eventID": "example4-6826-4c0a-bdec-0bab1example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

UntagResource

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:44:16Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UntagResource",

```

```

"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
"requestParameters": {
  "resourceArn": "arn:aws:rbn:us-west-2:123456789012:rule/ABCDEF01234",
  "tagKeys": [
    "purpose"
  ]
},
"responseElements": null,
"requestID": "example7-6c1e-4f09-9e46-bb957example",
"eventID": "example6-75ff-4c94-a1cd-4d5f5example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbn.us-west-2.amazonaws.com"
}
}

```

ListTagsForResource

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      }
    }
  },

```

```

    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-10-22T21:38:34Z"
    }
  },
  "eventTime": "2021-10-22T21:42:31Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListTagsForResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 boto3/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
  },
  "responseElements": null,
  "requestID": "example8-10c7-43d4-b147-3d9d9example",
  "eventID": "example2-24fc-4da7-a479-c9748example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}

```

LockRule

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {

```

```
"sessionIssuer": {
  "type": "Role",
  "principalId": "123456789012",
  "arn": "arn:aws:iam::123456789012:role/Admin",
  "accountId": "123456789012",
  "userName": "Admin"
},
"webIdFederationData": {},
"attributes": {
  "creationDate": "2022-10-25T00:45:11Z",
  "mfaAuthenticated": "false"
}
}
},
"eventTime": "2022-10-25T00:45:19Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "LockRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "python-requests/2.25.1",
"requestParameters": {
  "identifier": "jkrnexample",
  "lockConfiguration": {
    "unlockDelay": {
      "unlockDelayValue": 7,
      "unlockDelayUnit": "DAYS"
    }
  }
}
},
"responseElements": {
  "identifier": "jkrnexample",
  "description": "",
  "resourceType": "EBS_SNAPSHOT",
  "retentionPeriod": {
    "retentionPeriodValue": 7,
    "retentionPeriodUnit": "DAYS"
  }
},
"resourceTags": [],
"status": "available",
"lockConfiguration": {
  "unlockDelay": {
    "unlockDelayValue": 7,
    "unlockDelayUnit": "DAYS"
  }
}
```

```

    },
    "lockState": "locked"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}

```

UnlockRule

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-25T00:46:17Z",

```

```
"eventSource": "rbin.amazonaws.com",
"eventName": "UnlockRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "python-requests/2.25.1",
"requestParameters": {
  "identifier": "jkrnexample"
},
"responseElements": {
  "identifier": "jkrnexample",
  "description": "",
  "resourceType": "EC2_IMAGE",
  "retentionPeriod": {
    "retentionPeriodValue": 7,
    "retentionPeriodUnit": "DAYS"
  },
  "resourceTags": [],
  "status": "available",
  "lockConfiguration": {
    "unlockDelay": {
      "unlockDelayValue": 7,
      "unlockDelayUnit": "DAYS"
    }
  },
  "lockState": "pending_unlock",
  "lockEndTime": "Nov 1, 2022, 12:46:17 AM"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```

Emplacements des ressources

Les ressources Amazon EC2 sont spécifiques à la AWS région ou à la zone de disponibilité dans laquelle elles se trouvent.

Ressource	Type	Description
Identifiants de ressource Amazon EC2	Régional	Chaque identificateur de ressource (tel qu'un ID d'AMI, d'instance, de volume EBS ou d'instantané) est lié à sa région et peut être utilisé uniquement dans la région où vous avez créé la ressource.
Noms de ressource fournis par l'utilisateur	Régional	Chaque nom de ressource (comme un nom de groupe de sécurité ou de paire de clés) est lié à sa région et peut être utilisé uniquement dans la région où vous avez créé la ressource. Même si vous pouvez créer des ressources avec le même nom dans plusieurs régions, ces ressources ne sont pas liées.
AMI	Régional	Une AMI est liée à la région dans laquelle ses fichiers sont situés au sein d'Amazon S3. Vous pouvez copier une AMI d'une région à une autre. Pour plus d'informations, consultez Copier une AMI .
Instantanés EBS	Régional	Un instantané (snapshot) EBS est lié à sa région et peut être uniquement utilisé pour créer des volumes dans la même région. Vous pouvez copier un instantané d'une région à une autre.
Volumes EBS	Zone de disponibilité	Un volume Amazon EBS est lié à sa zone de disponibilité et peut être uniquement attaché à des instances de la même zone de disponibilité.
Adresses IP Elastic	Régional	Une adresse IP Elastic est liée à une région et ne peut être associée qu'à une instance de la même région.

Ressource	Type	Description
instances	Zone de disponibilité	Une instance est liée à la zone de disponibilité dans laquelle vous l'avez lancée. Cependant, son ID d'instance est lié à la région.
Paires de clés	Mondial ou régional	<p>Les paires de clés que vous créez à l'aide d'Amazon EC2 sont liées à la région où vous les avez créées. Vous pouvez créer votre propre paire de clés RSA et la télécharger dans la région dans laquelle vous voulez l'utiliser. Par conséquent, vous pouvez la mettre à disposition dans le monde entier en la téléchargeant dans chaque région.</p> <p>Pour plus d'informations, consultez Paires de clés Amazon EC2 et instances Amazon EC2.</p>
Groupes de sécurité	Régional	Un groupe de sécurité est lié à une région et ne peut être affecté qu'aux instances de la même région. Vous ne pouvez pas permettre à une instance de communiquer avec une instance se trouvant en dehors de sa région à l'aide de règles de groupe de sécurité. Le trafic provenant d'une instance située dans une autre région est considéré comme un trafic à bande passante de réseau étendu (WAN).

ID de ressource

Lorsque des ressources sont créées, nous affectons à chacune d'entre elles un ID de ressource unique. Un ID de ressource est constitué d'un identificateur de ressource (par exemple, snap pour un instantané) suivi d'un tiret et d'une combinaison unique de lettres et de chiffres.

Chaque identificateur de ressource (tel qu'un ID d'AMI, d'instance, de volume EBS ou d'instantané) est lié à sa région et peut être utilisé uniquement dans la région où vous avez créé la ressource.

Vous pouvez utiliser des ID de ressource pour rechercher vos ressources sur la console Amazon EC2. Si vous utilisez un outil de ligne de commande ou l'API Amazon EC2 pour gérer Amazon EC2, des ID de ressource sont requis pour certaines commandes. Par exemple, si vous utilisez la AWS CLI commande [stop-instances](#) pour arrêter une instance, vous devez spécifier l'ID de l'instance dans la commande.

Longueur des ID de ressource

Avant janvier 2016, les ID affectés aux ressources nouvellement créées de certains types de ressource utilisaient 8 caractères après le tiret (par exemple, i-1a2b3c4d). De janvier 2016 à juin 2018, nous avons modifié les ID de ces types de ressource pour utiliser 17 caractères après le tiret (par exemple, i-1234567890abcdef0). Selon le moment où votre compte a été créé, vous pouvez disposer de ressources existantes avec des ID courts, cependant toutes les nouvelles ressources reçoivent les ID longs.

Lister et filtrer vos ressources

Vous pouvez obtenir la liste de certains types de ressource à l'aide de la console Amazon EC2. Vous pouvez obtenir une liste de chaque type de ressource à l'aide de sa commande ou de son action d'API correspondante. Si vous avez plusieurs ressources, vous pouvez filtrer les résultats pour n'inclure ou n'exclure que les ressources qui correspondent à certains critères.

Sommaire

- [Lister et filtrer des ressources à l'aide de la console](#)
- [Lister et filtrer à l'aide de la CLI et de l'API](#)
- [Afficher les ressources entre Régions à l'aide d'Amazon EC2 Global View](#)

Lister et filtrer des ressources à l'aide de la console

Table des matières

- [Lister des ressources à l'aide de la console](#)
- [Filtrer des ressources à l'aide de la console](#)
 - [Filtres pris en charge](#)

Lister des ressources à l'aide de la console

Vous pouvez afficher les types de ressource Amazon EC2 les plus courants à l'aide de la console. Pour afficher des ressources supplémentaires, utilisez l'interface ligne de commande ou les actions d'API.

Pour afficher les ressources EC2 à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez l'option qui correspond à la ressource. Par exemple, pour créer une liste de vos instances, choisissez Instances.

La page affiche toutes les ressources du type de ressource sélectionné.

Filtrer des ressources à l'aide de la console

Pour filtrer une liste de ressources

1. Dans le panneau de navigation, sélectionnez un type de ressource (par exemple, Instances).
2. Choisissez le champ de recherche.
3. Sélectionnez le filtre dans la liste.
4. Sélectionnez un opérateur, par exemple, = (Equals (égal à)). Certains attributs ont plus d'opérateurs disponibles à sélectionner. Notez que tous les écrans ne prennent pas en charge la sélection d'un opérateur.
5. Sélectionnez une valeur de filtre.
6. Pour modifier un filtre sélectionné, choisissez le jeton de filtre (zone bleue), apportez les modifications requises, puis choisissez Appliquer. Notez que tous les écrans ne prennent pas en charge la modification du filtre sélectionné.

Search

Architecture = arm64

Name

Edit filter

Property Architecture

Operator =
Equals

Value arm64

Cancel Apply

7. Lorsque vous avez terminé, retirez le filtre.

Filtres pris en charge

La console Amazon EC2 prend en charge deux types de filtrage.

- Le filtrage des API se produit côté serveur. Le filtrage est appliqué à l'appel d'API qui réduit le nombre de ressources renvoyées par le serveur. Il permet un filtrage rapide sur des ensembles volumineux de ressources et peut réduire le temps et le coût du transfert de données entre le serveur et le navigateur. Filtrage d'API est compatible avec les opérateurs =(equals (égal à)) et :(contains (contient), et est toujours sensible à la casse.
- Le filtrage client se produit du côté du client. Il vous permet de filtrer les données déjà disponibles dans le navigateur (en d'autres termes, les données qui ont déjà été renvoyées par l'API). Le filtrage client fonctionne parfaitement en conjonction avec un filtre d'API de manière à réduire le filtrage à de plus petits ensembles de données dans le navigateur. En plus des opérateurs =(equals (égal à)) et :(contains (contient)) opérateurs, le filtrage client peut également prendre en charge les opérateurs de plage, tels que >=(greater than or equal (supérieur ou égal à)) et les opérateurs de négation (inverse), tels que !=(does not equal (n'est pas égal à)).

La console Amazon EC2 prend en charge les types de recherches suivants :

Recherche par mot-clé

La recherche par mot clé est une recherche de texte libre qui vous permet de rechercher une valeur parmi tous les attributs de vos ressources ou balises, sans spécifier l'attribut ou la balise à rechercher.

Note

Toutes les recherches par mots-clés utilisent le filtrage client.

Pour rechercher par mot-clé, entrez ou collez ce que vous recherchez dans la zone de recherche, puis choisissez Enter (Entrer). Par exemple, rechercher 123 établit la correspondance avec toutes les instances qui ont 123 dans l'un quelconque de leurs attributs, par exemple, une adresse IP, un ID d'instance, un ID de VPC ou un ID d'AMI, ou dans l'un quelconque de leurs balises telles que Nom. Si votre recherche de texte libre renvoie des correspondances inattendues, appliquez des filtres supplémentaires.

Recherche par attribut

La recherche par attribut vous permet de rechercher un attribut spécifique parmi toutes vos ressources.

Note

Les recherches par attribut utilisent le filtrage d'API ou le filtrage client, en fonction de l'attribut sélectionné. Lors d'une recherche par attribut, les attributs sont regroupés en conséquence.

Par exemple, vous pouvez rechercher l'attribut État de l'instance pour toutes vos instances afin de renvoyer uniquement les instances dont l'état est stopped. Pour cela :

1. Dans le champ de recherche de l'écran Instances, commencez à saisir Instance state. Au fur et à mesure que vous entrez les caractères, les deux types de filtres apparaissent pour État de l'instance : les filtres API et les filtres client.
2. Pour effectuer une recherche côté serveur, choisissez État de l'instance sous Filtres API. Pour effectuer une recherche côté client, choisissez État de l'instance (client) sous Filtres client.

Une liste d'opérateurs possibles pour l'attribut sélectionné s'affiche.

3. Cliquez sur l'onglet=opérateur (Equals (égal à)).

Une liste des valeurs possibles pour l'attribut et l'opérateur sélectionné s'affiche.

4. Sélectionnez Arrêté dans la liste.

Rechercher par identification

La recherche par balise permet de filtrer les ressources du tableau actuellement affiché par une clé de balise ou une valeur de balise.

Les recherches de balises utilisent soit Filtrage API ou filtrage client, selon les paramètres de la fenêtre Preferences (Préférences).

Pour garantir le filtrage des API pour les balises

1. Ouvrir l'onglet Preferences (Préférences).
2. Effacer la case Utiliser la mise en correspondance d'expressions régulières. Si cette case est cochée, le filtrage client est effectué.
3. Sélectionnez la case Correspondance avec respect des casse. Si cette case est cochée, le filtrage client est effectué.
4. Choisissez Confirmer.

Lorsque vous effectuez une recherche par balise, vous pouvez utiliser les valeurs suivantes :

- (vide)— Recherchez toutes les ressources avec la clé de balise spécifiée, mais il ne doit pas y avoir de valeur de balise.
- Toutes les valeurs— Recherchez toutes les ressources avec la clé de balise spécifiée et n'importe quelle valeur de balise.
- Non balisé – Pour rechercher toutes les ressources qui n'ont pas la clé de balise spécifiée.
- La valeur affichée : permet de rechercher toutes les ressources avec la clé de balise spécifiée et la valeur de balise spécifiée.

Vous pouvez utiliser les techniques suivantes pour améliorer ou affiner vos recherches.

Recherche inversée

Les recherches inverses vous permettent de rechercher des ressources qui ne correspondent pas à une valeur spécifiée. Dans les écrans Instances et AMI, les recherches inverses sont effectuées en sélectionnant l'opérateur != (Does not equal (N'est pas égal à)) ou !: (Does not contain (Ne

contient pas)), puis en sélectionnant une valeur. Dans d'autres écrans, les recherches inverses s'effectuent en préfixant le mot clé de recherche d'un caractère point d'exclamation (!).

 Note

La recherche inverse est prise en charge avec des recherches par mot-clé et des recherches par attribut uniquement sur des filtres client. Elle n'est pas prise en charge avec des recherches par attribut sur les filtres d'API.

Par exemple, vous pouvez rechercher l'attribut État de l'instance pour toutes vos instances afin de renvoyer uniquement les instances dont l'état est `terminated`. Pour cela :

1. Dans le champ de recherche de l'écran Instances, commencez à saisir `Instance state`. Au fur et à mesure que vous entrez les caractères, les deux types de filtres apparaissent pour État de l'instance : les filtres API et les filtres client.
2. Sous Filtres client, choisissez État de l'instance (client). La recherche inverse n'est prise en charge que sur les filtres client.

Une liste d'opérateurs possibles pour l'attribut sélectionné s'affiche.

3. Choisissez `!=(Does not equal (N'est pas égal à))`, puis choisissez `résilié`.

Pour filtrer les instances en fonction d'un attribut d'état d'instance, vous pouvez également utiliser les icônes de recherche (



) dans la colonne État de l'instance. L'icône de recherche avec un signe plus (+) affiche toutes les instances correspondant à cet attribut. L'icône de recherche avec un signe moins (-) exclut toutes les instances correspondant à cet attribut.

Voici un autre exemple d'utilisation de la recherche inverse : pour répertorier toutes les instances qui ne sont pas affectées au groupe de sécurité nommé `launch-wizard-1`, sous Filtres client, effectuez une recherche via l'attribut `Security group name` (Nom du groupe de sécurité), choisissez `!=`, et dans la barre de recherche entrez `launch-wizard-1`.

Recherche partielle

Avec les recherches partielles, vous pouvez rechercher des valeurs de chaîne partielles. Pour effectuer une recherche partielle, entrez uniquement une partie du mot-clé que vous souhaitez rechercher. Dans les écrans `Instances` et `AMI`, les recherches partielles ne peuvent être effectuées

qu'avec l'opérateur :(Contains (Contient)). Sur d'autres écrans, vous pouvez sélectionner l'attribut de filtre client et entrer immédiatement uniquement une partie du mot-clé que vous souhaitez rechercher. Par exemple, dans l'écran Type d'instance , pour rechercher toutes les instances , et `t2.micro`, effectuez une recherche par l'attribut `t2.smallInstance Type (Type d'instance)t2.medium` puis saisissez `t2`.

Recherche d'expression régulière

Pour utiliser les recherches d'expression régulière, vous devez sélectionner la case à cocher `Use regular expression matching (Utiliser la correspondance d'expression régulière)` dans la fenêtre `Preferences (préférences)`.

Les expressions régulières sont utiles quand vous avez besoin de faire correspondre les valeurs d'un champ à un modèle spécifique. Par exemple, pour rechercher une valeur qui commence par `s`, recherchez `^s`. Pour rechercher une valeur qui se termine par `xyz`, recherchez `xyz$`. Pour rechercher une valeur commençant par un nombre suivi d'un ou de plusieurs caractères, recherchez `[0-9]+.*`.

Note

La recherche par expression régulière est prise en charge avec les recherches par mot-clé et les recherches par attribut uniquement sur les filtres client. Elle n'est pas prise en charge avec des recherches par attribut sur les filtres d'API.

Recherche sensible à la casse

Pour utiliser des recherches sensibles à la casse, vous devez sélectionner le `Correspondance avec respect des casses` dans la fenêtre `Preferences (Préférences)`. La préférence sensible à la casse s'applique uniquement aux filtres des clients et des balises.

Note

Les filtres d'API sont toujours sensibles à la casse.

Recherche par caractère générique

Utilisez le caractère générique `*` pour faire correspondre zéro ou plusieurs caractères. Utilisez le caractère générique `?` pour faire correspondre zéro ou un caractère. Par exemple, si vous

disposez d'un ensemble de données contenant les valeurs `prod`, `prods`, et `production`, une recherche `deprod*` correspond à toutes les valeurs, tandis que `prod?` correspond uniquement à `prod` et `prods`. Pour utiliser les valeurs littérales, échappez-les avec une barre oblique inverse (`\`). Par exemple, `"prod\"*` correspondrait à `prod*`.

Note

La recherche par caractère générique est prise en charge avec les recherches par attribut et balise uniquement sur les filtres d'API. Elle n'est pas prise en charge avec les recherches par mot-clé et les recherches par attribut et balise uniquement sur les filtres client.

Combinaison de recherches

En général, plusieurs filtres avec le même attribut sont automatiquement joints avec OR. Par exemple, la recherche `Instance State : Running` et `Instance State : Stopped` renvoie toutes les instances en cours d'exécution OU arrêtées. Pour joindre la recherche avec AND, recherchez sur différents attributs. Par exemple, les recherches `Instance State : Running` et `Instance Type : c4.large` renvoient uniquement les instances de type `c4.large` ET qui sont dans l'état d'exécution.

Lister et filtrer à l'aide de la CLI et de l'API

Chaque type de ressource possède une commande de CLI ou une action d'API correspondante que vous utilisez pour afficher les ressources de ce type. Les listes de ressources qui en résultent peuvent être longues, de sorte qu'il peut être plus rapide et plus utile de filtrer les résultats pour inclure uniquement les ressources qui répondent à des critères spécifiques.

Considérations relatives au filtrage

- Vous pouvez spécifier jusqu'à 50 filtres et jusqu'à 200 valeurs par filtre en une seule demande.
- Les chaînes de filtre peuvent comporter jusqu'à 255 caractères.
- Vous pouvez aussi utiliser des caractères génériques avec les valeurs de filtre. Un astérisque (*) correspond à zéro ou plusieurs caractères, et un point d'interrogation (?) correspond à zéro ou un caractère.
- Les valeurs de filtre sont sensibles à la casse.

- Votre recherche peut inclure les valeurs littérales des caractères génériques ; vous devez simplement leur associer une séquence d'échappement avec une barre oblique inverse devant le caractère. Par exemple, la valeur `*amazon\?\` recherche la chaîne littérale `*amazon?\`.

Filtres pris en charge

Pour découvrir les filtres pris en charge pour chaque ressource Amazon EC2, consultez la documentation suivante :

- AWS CLI : commandes `describe` dans [AWS CLI Référence des commandes Amazon EC2](#).
- Outils pour Windows PowerShell : les `Get` commandes de l'[AWS Tools for PowerShell applet de commande Reference-Amazon](#) EC2.
- API de requête : les `Describe` actions des API dans [Référence des API Amazon EC2](#).

Exemple Exemple : spécifier un filtre unique

Vous pouvez lister vos instances Amazon EC2 à l'aide de la commande [describe-instances](#). Sans aucun filtre, la réponse contient les informations pour toutes vos ressources. Vous pouvez utiliser la commande suivante pour inclure uniquement les instances en cours d'exécution dans votre sortie.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running
```

Pour répertorier uniquement les ID des instances en cours d'exécution, ajoutez le paramètre `--query` comme suit.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running --query "Reservations[*].Instances[*].InstanceId" --output text
```

Voici un exemple de sortie.

```
i-0ef1f57f78d4775a4  
i-0626d4edd54f1286d  
i-04a636d18e83cfacb
```

Exemple Exemple : spécifier plusieurs filtres ou valeurs de filtre

Si vous spécifiez plusieurs filtres ou plusieurs valeurs de filtre, la ressource doit correspondre à tous les filtres pour pouvoir apparaître dans les résultats.

Vous pouvez utiliser la commande suivante pour répertorier toutes les instances dont le type est `m5.large` ou `m5d.large`.

```
aws ec2 describe-instances --filters Name=instance-type,Values=m5.large,m5d.large
```

Vous pouvez utiliser la commande suivante pour répertorier toutes les instances arrêtées dont le type est `t2.micro`.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=stopped
Name=instance-type,Values=t2.micro
```

Exemple Exemple : utiliser des caractères génériques dans une valeur de filtre

Si vous spécifiez `database` comme valeur de filtre pour le filtre `description` lors de la description des instantanés EBS via [describe-snapshots](#), la commande renvoie uniquement les instantanés dont la description correspond à « `database` ».

```
aws ec2 describe-snapshots --filters Name=description,Values=database
```

Le caractère générique `*` correspond à zéro ou plusieurs caractères. Si vous spécifiez `*database*` comme valeur de filtre, la commande renvoie uniquement les instantanés dont la description inclut ce terme.

```
aws ec2 describe-snapshots --filters Name=description,Values=*database*
```

Le caractère générique `?` correspond à 1 seul caractère. Si vous spécifiez `database?` comme valeur de filtre, la commande renvoie uniquement les instantanés dont la description correspond à « `database` » ou à ce terme, suivi d'un caractère.

```
aws ec2 describe-snapshots --filters Name=description,Values=database?
```

Si vous indiquez `database????`, la commande renvoie uniquement les instantanés dont la description correspond à « `database` », suivi d'un maximum de quatre caractères. Elle exclut les descriptions contenant le terme « `database` » suivi de cinq caractères ou plus.

```
aws ec2 describe-snapshots --filters Name=description,Values=database????
```

Exemple Exemple : filtre basé sur la date

Avec le AWS CLI, vous pouvez utiliser JMESPath pour filtrer les résultats à l'aide d'expressions.

Par exemple, la [describe-snapshots](#) commande suivante affiche les ID de tous les instantanés créés par votre Compte AWS (représenté par 123456789012) avant la date spécifiée (représentée par le 31/03/2020). Si vous ne spécifiez pas le propriétaire, les résultats incluent tous les instantanés publics.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

La commande suivante affiche les ID de tous les instantanés créés dans la plage de dates spécifiée.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]" --output text
```

Filtre basé sur les balises

Pour obtenir des exemples de filtrage d'une liste de ressources en fonction de leurs balises, consultez [Utiliser des balises à l'aide de la ligne de commande](#).

Afficher les ressources entre Régions à l'aide d'Amazon EC2 Global View

Amazon EC2 Global View vous permet de consulter et de rechercher des ressources Amazon EC2 et Amazon VPC dans AWS une seule région ou dans plusieurs régions simultanément sur une seule console. Pour plus d'informations, consultez [Amazon EC2 Global View \(Amazon EC2 Global View\)](#).

Amazon EC2 Global View (Amazon EC2 Global View)

Amazon EC2 Global View vous permet d'afficher certaines de vos ressources Amazon EC2 et Amazon VPC hébergées dans une Région AWS unique, ou dans plusieurs Régions sur une même console. Amazon EC2 Global View possède également une fonctionnalité global search (recherche globale) qui vous permet de rechercher simultanément des ressources spécifiques ou des types de ressources spécifiques dans plusieurs Régions.

Il est impossible de modifier les ressources avec Amazon EC2 Global View.

Ressources prises en charge

À l'aide d'Amazon EC2 Global View, vous pouvez consulter un résumé global des ressources suivantes dans toutes les régions pour lesquelles votre compte Compte AWS est activé.

- Groupes Auto Scaling
- Jeu d'options DHCP
- Passerelles Internet de sortie uniquement
- Adresses IP Elastic
- Services de point de terminaison
- instances
- Passerelles Internet
- Listes de préfixes gérées
- Passerelles NAT
- Listes ACL réseau
- Interfaces réseau
- Tables de routage
- Groupes de sécurité
- Sous-réseaux
- Volumes
- VPC
- Points de terminaison d'un VPC
- Connexions d'appairage de VPC

Autorisations nécessaires

Un utilisateur doit posséder les autorisations suivantes pour utiliser Amazon EC2 Global View.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeDhcpOptions",
```

```
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeAddresses",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribePrefixLists",
"ec2:DescribeNatGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVolumes",
"ec2:DescribeVpcs",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcPeeringConnections"
],
"Resource": "*"
}]
}
```

Pour utiliser Amazon EC2 Global View

Ouvrez la console Amazon EC2 Global View à l'adresse <https://console.aws.amazon.com/ec2globalview/home>.

 Important

Vous ne pouvez pas utiliser une fenêtre privée dans Firefox pour accéder à Amazon EC2 Global View.

La console comprend les éléments suivants :

- Region explorer (Explorateur de région). Cet onglet comprend les sections suivantes :
 - Synthèse : offre un aperçu général de vos ressources dans toutes les régions.

Les régions activées indiquent le nombre de régions pour lesquelles la vôtre Compte AWS est activée. Les champs restants indiquent le nombre de ressources dont vous disposez actuellement dans ces Régions. Sélectionnez l'un des liens pour afficher les ressources de ce type dans toutes les Régions. Par exemple, si le lien situé sous l'étiquette instances est 29 dans

10 Regions (29 dans 10 Régions), cela indique que vous avez actuellement 29 instances à travers 10 Régions. Cliquez sur ce lien pour afficher la liste des 29 instances.

- Nombre de régions de ressources : répertorie toutes les Régions AWS (y compris celles pour lesquelles votre compte n'est pas activé) et fournit des totaux pour chaque type de ressource pour chaque région.

Sélectionnez un nom de Région pour afficher toutes les ressources de tous les types pour cette Région donnée. Par exemple, sélectionnez Africa (Cape Town) af-south-1 (Afrique (Le Cap) af-south-1) pour afficher tous les VPC, les sous-réseaux, les instances, les groupes de sécurité, les volumes et les groupe Auto Scaling de cette Région. Vous pouvez également sélectionner une Région et sélectionner View resources for selected Region (Afficher les ressources pour la Région sélectionnée).

Sélectionnez la valeur d'un type de ressource spécifique dans une Région spécifique pour afficher uniquement les ressources de ce type dans cette Région. Par exemple, sélectionnez la valeur pour instances pour Africa (Cape Town) af-south-1 (Afrique (Le Cap) af-south-1) pour afficher uniquement les instances dans cette Région.

- Recherche globale : cet onglet vous permet de rechercher des ressources spécifiques ou des types de ressources spécifiques dans une seule région ou dans plusieurs régions. Il vous permet également d'afficher les détails d'une ressource spécifique.

Pour rechercher des ressources, entrez les critères de recherche dans le champ précédant la grille. Vous pouvez effectuer une recherche par Région, par type de ressource et par balises affectées aux ressources.

Pour afficher les détails d'une ressource spécifique, sélectionnez-la dans la grille. Vous pouvez également sélectionner l'ID ressource d'une ressource pour l'afficher dans sa console. Par exemple, sélectionnez un ID d'instance pour afficher cette instance dans la console Amazon EC2 ou choisissez un ID sous-réseau pour afficher ce sous-réseau dans la console Amazon VPC.

Tip

Si vous utilisez uniquement des Régions ou des types de ressources spécifiques, vous pouvez personnaliser Amazon EC2 Global View pour n'afficher que ces Régions et ces types de ressources. Pour personnaliser les Régions et les types de ressources affichés, dans le panneau de navigation, choisissez Paramètres, puis dans les onglets Ressources et

Régions, sélectionnez les Régions et les types de ressources que vous ne souhaitez pas voir apparaître dans Amazon EC2 Global View.

Baliser vos ressources Amazon EC2

Pour vous aider à gérer vos instances, images et autres ressources Amazon EC2, vous pouvez affecter vos propres métadonnées sous la forme de balises. Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Cette approche est utile lorsque vous avez de nombreuses ressources de même type. Elle vous permet d'identifier rapidement une ressource spécifique en fonction des balises que vous lui avez attribuées. Cette rubrique décrit les balises et vous montre comment les créer.

Warning

Les clés de balise et leurs valeurs sont renvoyées par différents appels d'API. Le fait de refuser l'accès à DescribeTags ne refuse pas automatiquement l'accès aux balises renvoyées par d'autres API. Nous vous recommandons de ne pas inclure de données sensibles dans vos balises.

Sommaire

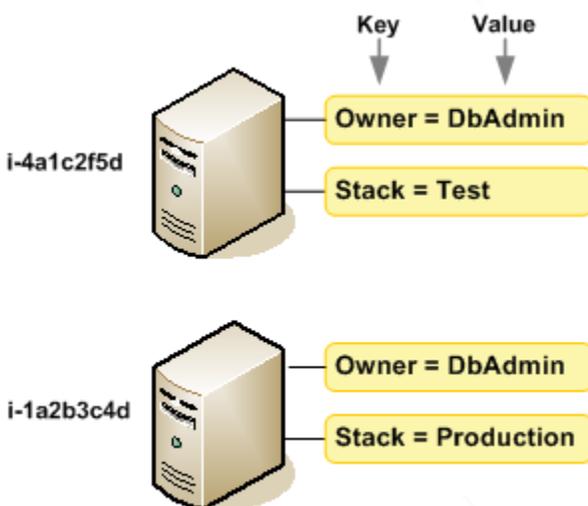
- [Principes de base des balises](#)
- [Etiqueter vos ressources](#)
- [Restrictions liées aux balises](#)
- [Gestion des balises et des accès](#)
- [Baliser vos ressources pour facturation](#)
- [Utiliser des balises à l'aide de la console](#)
- [Utiliser des balises à l'aide de la ligne de commande](#)
- [Utiliser les identifications d'instance dans les métadonnées d'instance](#)
- [Ajoutez des balises à une ressource à l'aide de CloudFormation](#)

Principes de base des balises

Une étiquette est une étiquette que vous attribuez à une AWS ressource. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez.

Les balises vous permettent de classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Par exemple, vous pouvez définir pour les instances de votre compte Amazon EC2 un ensemble de balises qui vous aide à suivre le propriétaire et le niveau de stack de chaque instance.

Le graphique suivant illustre le fonctionnement du balisage. Dans cet exemple, vous avez affecté deux balises à chacune de vos instances : une balise avec la clé `Owner` et une autre avec la clé `Stack`. Chaque balise possède également une valeur associée.



Nous vous recommandons de concevoir un ensemble de clés de balise répondant à vos besoins pour chaque type de ressource. L'utilisation d'un ensemble de clés de balise cohérent facilite la gestion de vos ressources. Vous pouvez rechercher et filtrer les ressources en fonction des étiquettes que vous ajoutez. Pour plus d'informations sur la mise en œuvre d'une stratégie de balisage des ressources efficace, consultez le livre blanc sur les [meilleures pratiques AWS en matière de balisage](#).

Les balises n'ont pas de signification sémantique pour Amazon EC2 et sont interprétées strictement comme des chaînes de caractères. De plus, les balises ne sont pas automatiquement affectées à vos ressources. Vous pouvez modifier les clés et valeurs de balise, et vous pouvez retirer des balises d'une ressource à tout moment. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur null. Si vous ajoutez une balise ayant la même

clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur. Si vous supprimez une ressource, ses balises sont également supprimées.

Note

Après avoir supprimé une ressource, il est possible que ses balises restent visibles pendant une courte période dans les sorties API et CLI de la console. Ces balises seront progressivement dissociées de la ressource et seront définitivement supprimées.

Etiqueter vos ressources

Vous pouvez attribuer des balises à la plupart des ressources Amazon EC2 qui existent déjà dans votre compte. Le [tableau](#) ci-dessous répertorie les ressources qui prennent en charge l'identification.

Si vous utilisez la console Amazon EC2, vous pouvez appliquer des balises aux ressources en utilisant l'onglet Tags sur l'écran des ressources correspondant, ou vous pouvez utiliser l'éditeur de balises de la AWS Resource Groups console. Certains écrans de ressource vous permettent de spécifier des balises pour une ressource lors de la création de cette ressource ; par exemple, une balise avec une clé de Name et une valeur que vous indiquez. Dans la plupart des cas, la console applique les balises immédiatement après la création de la ressource (plutôt qu'au cours de la création de ressources). La console peut organiser des ressources en fonction de la balise Name, mais cette balise n'a pas de signification sémantique pour le service Amazon EC2.

Si vous utilisez l'API Amazon EC2, le ou un AWS SDK AWS CLI, vous pouvez utiliser l'action d'API `CreateTags EC2` pour appliquer des balises aux ressources existantes. En outre, certaines actions de création de ressources vous permettent de spécifier des balises pour une ressource lors de la création de cette dernière. Si les balises ne peuvent pas être appliquées au cours de la création de ressources, nous restaurons le processus de création de ressources. Cela permet de s'assurer que les ressources sont créées avec des balises ou qu'elles ne sont pas créées du tout, et qu'aucune ressource ne demeure sans balise à tout moment. En attribuant des balises aux ressources au moment de la création, vous pouvez supprimer la nécessité d'exécuter des scripts de balisage personnalisés après la création de ressources. Pour plus d'informations sur la façon de permettre aux utilisateurs de baliser des ressources lors de la création, consultez [Accorder l'autorisation de baliser les ressources lors de la création](#).

Le tableau suivant décrit les ressources Amazon EC2 qui peuvent être balisées et les ressources qui peuvent être balisées lors de leur création à l'aide de l'API Amazon EC2, AWS CLI du ou d'un SDK.

AWS

Prise en charge du balisage pour les ressources Amazon EC2

Ressource	Prend en charge les balises	Prend en charge le balisage au moment de la création
AFI	Oui	Oui
AMI	Oui	Oui
Tâche de bundle	Non	Non
Capacity Reservation	Oui	Oui
Passerelle transporteur	Oui	Oui
Point de terminaison VPN Client	Oui	Oui
Route VPN Client	Non	Non
Passerelle client	Oui	Oui
Dedicated Host	Oui	Oui
Réservation Hôte dédié	Oui	Oui
Options DHCP	Oui	Oui
Instantané EBS	Oui	Oui
Volume EBS	Oui	Oui
EC2 Fleet	Oui	Oui
Passerelle Internet de sortie uniquement	Oui	Oui
Adresse IP Elastic	Oui	Oui
Accélérateur Elastic Graphics	Oui	Non
Instance	Oui	Oui

Ressource	Prend en charge les balises	Prend en charge le balisage au moment de la création
Fenêtre d'événement de l'instance	Oui	Oui
Volume de stockage d'instance	N/A	N/A
Passerelle Internet	Oui	Oui
Pool d'adresses IP (BYOIP)	Oui	Oui
Paire de clés	Oui	Oui
Modèle de lancement	Oui	Oui
Version du modèle de lancement	Non	Non
Passerelle locale	Oui	Non
Table de routage de passerelle locale	Oui	Non
Interface virtuelle de passerelle locale	Oui	Non
Groupe d'interface virtuelle de passerelle locale	Oui	Non
Association de VPC de table de routage de passerelle locale	Oui	Oui
Association de groupe d'interface virtuelle de table de routage de passerelle locale	Oui	Non
Passerelle NAT	Oui	Oui

Ressource	Prend en charge les balises	Prend en charge le balisage au moment de la création
ACL réseau	Oui	Oui
Interface réseau	Oui	Oui
Groupe de placement	Oui	Oui
Listes de préfixes	Oui	Oui
Reserved Instance	Oui	Non
Liste d'entités d'Instance réservée	Non	Non
Table de routage	Oui	Oui
Demande de parc d'instances Spot	Oui	Oui
Demande d'instance Spot	Oui	Oui
Groupe de sécurité	Oui	Oui
Règle de groupe de sécurité	Oui	Non
Sous-réseau	Oui	Oui
Filtre Traffic Mirror	Oui	Oui
Session Traffic Mirror	Oui	Oui
Cible Traffic Mirror	Oui	Oui
Passerelle de transit	Oui	Oui
Domaine multicast de passerelle de transit	Oui	Oui

Ressource	Prend en charge les balises	Prend en charge le balisage au moment de la création
Table de routage de passerelle de transit	Oui	Oui
Attachement de VPC de passerelle de transit	Oui	Oui
Passerelle réseau privé virtuel	Oui	Oui
VPC	Oui	Oui
Point de terminaison d'un VPC	Oui	Oui
Service de point de terminaison d'un VPC	Oui	Oui
Configuration de service de point de terminaison de VPC	Oui	Oui
Journal de flux VPC	Oui	Oui
Connexion d'appairage de VPC	Oui	Oui
Connexion VPN	Oui	Oui

Vous pouvez baliser les instances, les volumes, les graphiques élastiques, les interfaces réseau et les demandes d'instance Spot lors de la création à l'aide de l'[assistant de lancement d'instance](#) Amazon EC2 dans la console Amazon EC2. Vous pouvez baliser vos volumes EBS au moment de leur création en utilisant l'écran Volumes, ou les instantanés EBS dans l'écran Instantanés. Vous pouvez également utiliser les API Amazon EC2 qui créent des ressources (par exemple [RunInstances](#)) pour appliquer des balises lors de la création de votre ressource.

Vous pouvez appliquer des autorisations au niveau des ressources basées sur des balises dans vos politiques IAM aux actions d'API Amazon EC2 qui prennent en charge le balisage à la création, afin de mettre en œuvre un contrôle détaillé des utilisateurs et des groupes qui peuvent baliser des ressources à leur création. Vos ressources sont correctement sécurisées depuis la création. Les

balises sont appliquées immédiatement à vos ressources. Les autorisations de niveau ressource basées sur des balises sont donc effectives immédiatement. Vos ressources peuvent être suivies et signalées avec plus de précision. Vous pouvez appliquer l'utilisation du balisage sur les nouvelles ressources et contrôler que les clés et valeurs de balise sont définies sur vos ressources.

Vous pouvez également appliquer des autorisations au niveau des ressources pour les actions d'API Amazon EC2 `CreateTags` et `DeleteTags` dans vos stratégies IAM afin de contrôler les clés et valeurs de balise définies sur vos ressources existantes. Pour plus d'informations, veuillez consulter [Exemple : Baliser des ressources](#).

Pour plus d'informations sur l'étiquetage de vos ressources pour la facturation, consultez [Utilisation des étiquettes de répartition des coûts](#) dans le AWS Billing Guide de l'utilisateur.

Restrictions liées aux balises

Les restrictions de base suivantes s'appliquent aux balises :

- Nombre maximal de balises par ressource : 50
- Pour chaque ressource, chaque clé de balise doit être unique, et chaque clé de balise peut avoir une seule valeur.
- Longueur de clé maximale : 128 caractères Unicode en UTF-8
- Longueur de valeur maximale : 256 caractères Unicode en UTF-8
- Caractères autorisés
 - Bien qu'EC2 autorise n'importe quel caractère dans ses balises, d'autres AWS services sont plus restrictifs. Les caractères autorisés dans tous les AWS services sont : les lettres (a-z,A-Z), les chiffres (0-9) et les espaces représentables en UTF-8, ainsi que les caractères suivants : . + - = . _ : / @
 - Si vous activez les identifications d'instance dans les métadonnées d'instance, les clés d'identification d'instance ne peuvent utiliser que des lettres (a-z, A-Z), des nombres (0-9), ainsi que les caractères suivants : + - = . , _ : @. Les clés d'identification des instances ne peuvent pas contenir d'espaces ou de /, et ne peuvent pas comprendre uniquement . (un point), .. (deux points) ou `_index`. Pour plus d'informations, consultez [Utiliser les identifications d'instance dans les métadonnées d'instance](#).
- Les clés et valeurs d'étiquette sont sensibles à la casse.
- Le `aws :` préfixe est réservé à l' AWS usage. Lorsque la balise possède une clé de balise avec ce préfixe, vous ne pouvez pas modifier ou supprimer sa clé ou sa valeur. Les balises avec le préfixe `aws :` ne sont pas comptabilisées comme vos balises pour la limite de ressources.

Vous ne pouvez pas mettre fin à une ressource, ou l'arrêter ou la supprimer uniquement en fonction de ses balises ; vous devez spécifier l'identificateur de ressource. Par exemple, pour supprimer des instantanés (snapshot) que vous avez balisés avec une clé de balise appelée `DeleteMe`, vous devez utiliser l'action `DeleteSnapshots` avec les identificateurs de ressource des instantanés, tels que `snap-1234567890abcdef0`.

Lorsque vous balisez des ressources publiques ou partagées, les balises que vous attribuez ne sont disponibles que pour votre AWS compte ; aucun autre AWS compte n'a accès à ces balises. Pour le contrôle d'accès basé sur des balises aux ressources partagées, chaque AWS compte doit attribuer son propre ensemble de balises pour contrôler l'accès à la ressource.

Vous ne pouvez pas attribuer des balises à toutes les ressources. Pour plus d'informations, veuillez consulter [Prise en charge du balisage pour les ressources Amazon EC2](#).

Gestion des balises et des accès

Si vous utilisez AWS Identity and Access Management (IAM), vous pouvez contrôler quels utilisateurs de votre AWS compte sont autorisés à créer, modifier ou supprimer des tags. Pour plus d'informations, consultez [Accorder l'autorisation de baliser les ressources lors de la création](#).

Vous pouvez également utiliser des balises de ressource pour implémenter le contrôle basé sur les attributs (ABAC). Vous pouvez créer des politiques IAM qui autorisent les opérations basées sur les balises de la ressource. Pour plus d'informations, veuillez consulter [Contrôler l'accès aux ressources EC2 à l'aide des balises de ressources](#).

Baliser vos ressources pour facturation

Vous pouvez utiliser des balises pour organiser votre AWS facture afin de refléter votre propre structure de coûts. Pour ce faire, inscrivez-vous pour obtenir la facture de votre AWS compte avec les valeurs clés du tag incluses. Pour plus d'informations sur la configuration d'un rapport de répartition des coûts avec des étiquettes, consultez [Rapport de répartition des coûts mensuel](#) dans le Guide de l'utilisateur AWS Billing . Pour voir le coût de vos ressources combinées, vous pouvez organiser vos informations de facturation en fonction des ressources possédant les mêmes valeurs de clé d'étiquette. Par exemple, vous pouvez baliser plusieurs ressources avec un nom d'application spécifique, puis organiser vos informations de facturation pour afficher le coût total de cette application dans plusieurs services. Pour plus d'informations, veuillez consulter [Utilisation des étiquettes de répartition des coûts](#) dans le AWS Billing Guide de l'utilisateur.

Note

Si vous venez d'activer la création de rapports, les données du mois en cours peuvent être consultées après 24 heures.

Les balises de répartition des coûts peuvent indiquer quelles ressources contribuent aux coûts, mais la suppression ou la désactivation des ressources ne réduit pas toujours les coûts. Par exemple, des données d'instantané qui sont référencées par un autre instantané sont conservées, même si l'instantané qui contient les données d'origine est supprimé. Pour plus d'informations, consultez [Volumes et instantanés Amazon Elastic Block Store](#) dans le AWS Billing Guide de l'utilisateur.

Note

Les adresses IP Elastic étiquetées ne sont pas affichées dans votre rapport de répartition des coûts.

Utiliser des balises à l'aide de la console

Vous pouvez utiliser la console Amazon EC2 pour afficher les balises d'une ressource individuelle, et pour appliquer ou supprimer les balises d'une ressource à la fois.

Vous pouvez utiliser l'éditeur de balises de la AWS Resource Groups console pour afficher les balises de toutes vos ressources Amazon EC2 dans toutes les régions. Vous pouvez afficher les balises par ressource et par type de ressource, et vous pouvez voir quels types de ressources sont associés à une balise donnée. Vous pouvez appliquer ou supprimer des balises pour plusieurs ressources et plusieurs types de ressources à la fois. L'éditeur de balises permet de centraliser et d'unifier la création et la gestion de vos balises. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS des ressources de balisage](#).

Tâches

- [Afficher des balises](#)
- [Ajouter et supprimer des balises pour une ressource individuelle](#)
- [Ajout et suppression de balises pour plusieurs ressources](#)
- [Ajouter une balise lorsque vous lancez une instance](#)
- [Filtrer une liste de ressources par balise](#)

Afficher des balises

Vous pouvez afficher les balises d'une ressource individuelle dans la console Amazon EC2. Pour afficher les balises de toutes vos ressources, utilisez l'éditeur de balises de la console AWS Resource Groups .

Affichage des balises d'une ressource individuelle

Lorsque vous sélectionnez une page spécifique d'une ressource sur la console Amazon EC2, celle-ci affiche une liste de ces ressources. Par exemple, si vous sélectionnez Instances dans le panneau de navigation, la console affiche une liste d'instances Amazon EC2. Lorsque vous sélectionnez une ressource dans l'une de ces listes (par exemple, un instance), si la ressource prend en charge les balises, vous pouvez afficher et gérer ses balises. Sur la plupart des pages de ressources, vous pouvez afficher les étiquettes en sélectionnant l'onglet Tags (étiquettes).

Vous pouvez ajouter une colonne à la liste des ressources pour afficher toutes les valeurs des balises ayant la même clé. Vous pouvez utiliser cette colonne pour trier et filtrer la liste des ressources par balise.

New console

Pour ajouter une colonne à la liste des ressources afin d'afficher vos balises

1. Dans la console EC2, cliquez sur l'icône en forme d'engrenage Préférences dans le coin supérieur droit de l'écran.
2. Dans la boîte de dialogue Préférences, sous Colonnes de balises (en bas à gauche), sélectionnez une ou plusieurs clés de balises, puis cliquez sur Confirmer.

Old console

Vous pouvez ajouter à la liste des ressources une nouvelle colonne pour afficher vos balises de deux manières.

- Dans l'onglet Balises, sélectionnez Afficher la colonne. Une nouvelle colonne est alors ajoutée à la console.
- Choisissez l'icône en forme d'engrenage Afficher / Masquer les colonnes puis, dans la boîte de dialogue Afficher / Masquer les colonnes, sélectionnez la clé de balise sous Vos clés de balise.

Affichage des balises pour plusieurs ressources

Vous pouvez afficher les balises de plusieurs ressources à l'aide de l'éditeur de balises de la [console AWS Resource Groups](#). Pour plus d'informations, consultez le [Guide de l'utilisateur AWS des ressources de balisage](#).

Ajouter et supprimer des balises pour une ressource individuelle

Vous pouvez gérer les balises pour une ressource individuelle directement à partir de la page de la ressource.

Pour ajouter une balise à une ressource individuelle

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région où se trouve la ressource à baliser. Pour plus d'informations, consultez [Emplacements des ressources](#).
3. Dans le panneau de navigation, sélectionnez un type de ressource (par exemple, Instances).
4. Sélectionnez la ressource à partir de la liste des ressources et choisissez l'onglet Balises.
5. Choisissez Gérer les balises, puis Ajouter une nouvelle balise. Entrez la clé et la valeur de la balise. Choisissez à nouveau Ajouter une nouvelle balise pour chaque balise supplémentaire à ajouter. Lorsque vous avez terminé d'ajouter des balises, choisissez Enregistrer.

Pour supprimer une balise d'une ressource individuelle

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région où se trouve la ressource dont la balise doit être supprimée. Pour plus d'informations, consultez [Emplacements des ressources](#).
3. Dans le panneau de navigation, sélectionnez un type de ressource (par exemple, Instances).
4. Sélectionnez la ressource à partir de la liste des ressources et choisissez l'onglet Balises.
5. Choisissez Manage tags (Gérer les balises). Pour chaque balise à supprimer, choisissez Supprimer. Lorsque vous avez terminé de supprimer des balises, choisissez Enregistrer.

Ajout et suppression de balises pour plusieurs ressources

Pour ajouter une balise à plusieurs ressources

1. Ouvrez l'éditeur de balises dans la console AWS Resource Groups à l'adresse <https://console.aws.amazon.com/resource-groups/tag-editor>.

2. Pour Régions, sélectionnez une ou plusieurs régions où se trouvent les ressources à baliser.
3. Pour les types de ressources, sélectionnez le type de ressources à étiqueter (par exemple, AWS::EC2::Instance).
4. Choisissez Rechercher des ressources.
5. Dans Résultats de la recherche de ressources, activez la case à cocher en regard de chaque ressource à baliser.
6. Choisissez Gérer les balises des ressources sélectionnées.
7. Dans Modifier les balises de toutes les ressources sélectionnées, choisissez Ajouter une balise, puis saisissez la nouvelle clé et la nouvelle valeur de la balise. Choisissez Add tag (Ajouter une identification) pour chaque étiquette supplémentaire.

 Note

Si vous ajoutez une nouvelles balise ayant la même clé de balise qu'une balise existante, la nouvelle balise remplace l'ancienne balise.

8. Choisissez Vérifier et appliquer les modifications apportées à la balise.
9. Choisissez Apply changes to all selected (Appliquer les modifications à tous les éléments sélectionnés).

Pour supprimer une balise de plusieurs ressources

1. Ouvrez l'éditeur de balises dans la console AWS Resource Groups à l'[adresse https://console.aws.amazon.com/resource-groups/tag-editor](https://console.aws.amazon.com/resource-groups/tag-editor).
2. Pour Régions, sélectionnez les régions où se trouvent les ressources dont la balise doit être supprimée.
3. Pour les types de ressources, sélectionnez le type de ressources à débaliser (par exemple, AWS::EC2::Instance).
4. Choisissez Rechercher des ressources.
5. Dans Résultats de la recherche de ressources, activez la case à cocher en regard de chaque ressource dont la balise doit être supprimée.
6. Choisissez Gérer les balises des ressources sélectionnées.
7. Sous Modifier les balises de toutes les ressources sélectionnées, à côté de la balise à supprimer, choisissez Supprimer la balise.

8. Choisissez Vérifier et appliquer les modifications apportées à la balise.
9. Choisissez Apply changes to all selected (Appliquer les modifications à tous les éléments sélectionnés).

Ajouter une balise lorsque vous lancez une instance

New console

Pour ajouter une balise à l'aide de l'assistant de lancement d'instance

1. À partir de la barre de navigation, sélectionnez la région souhaitée pour l'instance. Ce choix est important car certaines ressources Amazon EC2 peuvent être partagées entre des régions, contrairement à d'autres ressources. Sélectionnez la région qui répond à vos besoins. Pour plus d'informations, veuillez consulter [Emplacements des ressources](#).
2. Sélectionnez Launch instance (Lancer une instance).
3. Sous Name and tags (Noms et balises), vous pouvez saisir un nom descriptif pour votre instance et spécifier des balises.

Le nom de l'instance est une identification, où la clé est Name (Nom), et la valeur est le nom que vous spécifiez. Vous pouvez baliser l'instance, les volumes, les graphiques élastiques et les interfaces réseau. Pour les instances Spot, vous pouvez baliser uniquement la demande d'instance Spot.

La spécification d'un nom d'instance et d'identifications supplémentaires est facultative.

- Pour Name (Nom), saisissez un nom descriptif pour l'instance. Si vous ne spécifiez pas de nom, l'instance peut être identifiée par son ID, qui est automatiquement généré lorsque vous lancez l'instance.
 - Pour ajouter des identifications supplémentaires, sélectionnez Add additional tags (Ajouter des identifications supplémentaires). Choisissez Add tag (Ajouter une identification), saisissez une clé et une valeur, puis sélectionnez le type de ressource à étiqueter. Choisissez Add tag (Ajouter une identification) pour chaque étiquette supplémentaire.
4. Sous Application and OS Images (Amazon Machine Image) (Images d'applications et de systèmes d'exploitation [Amazon Machine Image]), sélectionnez le système d'exploitation de votre instance et une AMI. Pour plus d'informations, consultez [Images d'applications et de systèmes d'exploitation \(Amazon Machine Image\)](#).

5. Sous Key pair (login) (Paire de clés (connexion)), pour Key pair name (Nom de la paire de clés), choisissez une paire de clés existante ou créez-en une.
6. Conservez les valeurs par défaut de tous les autres champs ou choisissez des valeurs spécifiques pour la configuration d'instance souhaitée. Pour obtenir des informations sur les champs, consultez [Lancer une instance à l'aide de paramètres définis](#).
7. Dans le panneau Summary (Résumé), vérifiez vos paramètres, puis choisissez Launch instance (Lancer l'instance).

Old console

Pour ajouter une balise à l'aide de l'assistant de lancement d'instance

1. À partir de la barre de navigation, sélectionnez la région souhaitée pour l'instance. Ce choix est important car certaines ressources Amazon EC2 peuvent être partagées entre des régions, contrairement à d'autres ressources. Sélectionnez la région qui répond à vos besoins. Pour plus d'informations, veuillez consulter [Emplacements des ressources](#).
2. Choisissez Launch Instances.
3. La page Sélection d'une Amazon Machine Image (AMI) affiche une liste de configurations de base appelées Amazon Machine Images (AMIs). Sélectionnez l'AMI à utiliser, puis Sélectionner. Pour plus d'informations, veuillez consulter [Rechercher une AMI](#).
4. Sur la page Configurer les détails de l'instance, configurez les paramètres d'instance requis, puis cliquez sélectionnez Next: Add Storage (Suivant : Ajouter le stockage).
5. Sur la page Ajouter le stockage, vous pouvez spécifier des volumes de stockage supplémentaires pour votre instance. Choisissez Next: Add Tags (Suivant : Ajouter des balises) une fois que vous avez terminé.
6. Sur la page Ajouter des balises, spécifiez des balises pour l'instance, les volumes ou les deux. Choisissez Ajouter une autre balise pour ajouter plusieurs balises à votre instance. Choisissez Suivant : Configurer le groupe de sécurité une fois que vous avez terminé.
7. Sur la page Configurer le groupe de sécurité, vous pouvez sélectionner un groupe de sécurité existant parmi ceux que vous possédez ou laisser l'assistant créer un groupe de sécurité pour vous. Choisissez Vérifier et lancer lorsque vous avez terminé.
8. Vérifiez vos paramètres. Lorsque vous êtes satisfait de vos sélections, sélectionnez Lancer. Sélectionnez une paire de clés existante ou créez-en une, cochez la case de confirmation, puis cliquez sur Lancer des instances.

Filtrer une liste de ressources par balise

Vous pouvez filtrer votre liste de ressources selon une ou plusieurs clés de balise et valeurs de balise.

Pour filtrer une liste de ressources par balise dans la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez un type de ressource (par exemple, Instances).
3. Choisissez le champ de recherche.
4. Dans la liste, sous Balises, choisissez la clé de balise.
5. Choisissez la valeur de balise correspondante dans la liste.
6. Lorsque vous avez terminé, retirez le filtre.

Pour plus d'informations sur l'utilisation des filtres dans la console Amazon EC2, consultez [Lister et filtrer vos ressources](#).

Pour filtrer plusieurs ressources dans plusieurs régions par balise à l'aide de l'éditeur de balises

Vous pouvez utiliser l'éditeur de balises de la console AWS Resource Groups pour filtrer plusieurs ressources dans plusieurs régions par balise. Pour plus d'informations, consultez [Recherche de ressources à baliser](#) dans le Guide de l'utilisateur de Balisage des ressources AWS .

Utiliser des balises à l'aide de la ligne de commande

Vous pouvez ajouter des balises à de nombreuses ressources EC2 lors de leur création en utilisant le paramètre de spécifications de balise pour la commande créer. Vous pouvez afficher les balises d'une ressource à l'aide de la commande décrire de la ressource. Vous pouvez également ajouter, mettre à jour ou supprimer des balises pour vos ressources existantes à l'aide des commandes suivantes.

Tâche	AWS CLI	AWS Tools for Windows PowerShell
Ajouter ou remplacer une ou plusieurs balises	create-tags	New-EC2Tag
Supprimer une ou plusieurs balises.	delete-tags	Remove-EC2Tag

Tâche	AWS CLI	AWS Tools for Windows PowerShell
Décrire une ou plusieurs balises.	describe-tags	Get-EC2Tag

Tâches

- [Ajouter des balises lors de la création de ressources](#)
- [Ajouter des balises à une ressource existante](#)
- [Décrire les ressources balisées](#)

Ajouter des balises lors de la création de ressources

Les exemples suivants montrent comment appliquer des balises lorsque vous créez des ressources.

Note

La manière dont vous entrez des paramètres au format JSON sur la ligne de commande varie selon le système d'exploitation.

- Linux, macOS ou Unix et Windows PowerShell : utilisez des guillemets simples (') pour entourer la structure de données JSON.
- Windows : omettez les guillemets simples lorsque vous utilisez les commandes depuis la ligne de commande Windows.

Pour plus d'informations, consultez [Spécification de valeurs de paramètre pour l' AWS CLI](#).

Exemple Exemple : Lancez une instance et appliquez des balises à l'instance et au volume

La commande [run-instances](#) lance une instance et applique une balise avec une clé **webserver** et une valeur de **production** à cette dernière. La commande applique également une balise avec une clé de **cost-center** et une valeur **cc123** à n'importe quel volume EBS qui est créé (dans ce cas, le volume racine).

```
aws ec2 run-instances \  
  --image-id ami-abc12345 \  
  --count 1 \  
  --tag-specifications 'ResourceType=instance,Tags=[{Key=webserver,Value=production}]{Key=cost-center,Value=cc123}'
```

```
--instance-type t2.micro \  
--key-name MyKeyPair \  
--subnet-id subnet-6e7f829e \  
--tag-specifications  
'ResourceType=instance,Tags=[{Key=webserver,Value=production}]'  
'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Vous pouvez appliquer les mêmes clés et valeurs de balise aux instances et aux volumes pendant le lancement. La commande suivante lance une instance et applique une balise avec une clé de **cost-center** et une valeur de **cc123** à l'instance et à n'importe quel volume EBS qui est créé.

```
aws ec2 run-instances \  
  --image-id ami-abc12345 \  
  --count 1 \  
  --instance-type t2.micro \  
  --key-name MyKeyPair \  
  --subnet-id subnet-6e7f829e \  
  --tag-specifications 'ResourceType=instance,Tags=[{Key=cost-center,Value=cc123}]'  
'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Exemple Exemple : Créez un volume et appliquez une balise

La commande [create-volume](#) crée un volume et applique deux balises : **purpose=production**, et **cost-center=cc123**.

```
aws ec2 create-volume \  
  --availability-zone us-east-1a \  
  --volume-type gp2 \  
  --size 80 \  
  --tag-specifications 'ResourceType=volume,Tags=[{Key=purpose,Value=production},  
{Key=cost-center,Value=cc123}]'
```

Ajouter des balises à une ressource existante

Les exemples suivants montrent comment ajouter des balises à une ressource existante à l'aide de la commande [create-tags](#).

Exemple Exemple : Ajout d'une balise à une ressource

La commande suivante ajoute la balise **Stack=production** à l'image spécifiée ou remplace une balise existante pour l'AMI où la clé de balise est **Stack**. Si la commande réussit, aucune sortie n'est renvoyée.

```
aws ec2 create-tags \  
  --resources ami-78a54011 \  
  --tags Key=Stack,Value=production
```

Exemple Exemple : Ajout de balises à plusieurs ressources

Cet exemple ajoute (ou remplace) deux balises pour une AMI et une instance. L'une des balises contient simplement une clé (**webserver**), sans valeur (nous avons défini une chaîne vide comme valeur). L'autre balise est constituée d'une clé (**stack**) et d'une valeur (**Production**). Si la commande réussit, aucune sortie n'est renvoyée.

```
aws ec2 create-tags \  
  --resources ami-1a2b3c4d i-1234567890abcdef0 \  
  --tags Key=webserver,Value= Key=stack,Value=Production
```

Exemple Exemple : Ajout de balises avec des caractères spéciaux

Cet exemple ajoute la balise **[Group]=test** à une instance. Les crochets (**[** et **]**) sont des caractères spéciaux, qui doivent être échappés.

Si vous utilisez Linux ou OS X, pour échapper les caractères spéciaux, placez l'élément avec le caractère spécial entre des guillemets doubles ("), puis placez toute la structure de clé et de valeur entre des guillemets simples (').

```
aws ec2 create-tags \  
  --resources i-1234567890abcdef0 \  
  --tags 'Key="[Group]",Value=test'
```

Si vous utilisez Windows, pour échapper les caractères spéciaux, placez l'élément qui a des caractères spéciaux entre des guillemets doubles ("), puis faites précéder chaque guillemet double d'une barre oblique inverse (\), comme suit :

```
aws ec2 create-tags ^  
  --resources i-1234567890abcdef0 ^  
  --tags Key="[Group]",Value=test
```

Si vous utilisez Windows PowerShell, pour éviter les caractères spéciaux, placez la valeur contenant des caractères spéciaux entre guillemets ("), faites précéder chaque guillemet d'une barre oblique inverse (\), puis placez l'ensemble de la structure des clés et des valeurs entre guillemets simples (') comme suit :

```
aws ec2 create-tags \  
  --resources i-1234567890abcdef0 \  
  --tags 'Key=\"[Group]\",Value=test'
```

Décrire les ressources balisées

Les exemples suivants montrent comment utiliser des filtres avec [describe-instances](#) pour afficher des instances avec des balises spécifiques. Toutes les commandes décrire EC2 utilisent cette syntaxe pour filtrer par balise sur un seul type de ressource. Vous pouvez également utiliser la commande [describe-tags](#) pour filtrer par balise sur les types de ressources EC2.

Exemple Exemple : Décrire les instances avec la clé de balise spécifiée

La commande suivante décrit les instances avec une balise **Stack**, quelle que soit la valeur de la balise.

```
aws ec2 describe-instances \  
  --filters Name=tag-key,Values=Stack
```

Exemple Exemple : Décrire les instances avec la balise spécifiée

La commande suivante décrit les instances avec la balise **Stack=production**.

```
aws ec2 describe-instances \  
  --filters Name=tag:Stack,Values=production
```

Exemple Exemple : Décrire les instances avec la valeur de balise spécifiée

La commande suivante décrit les instances à l'aide d'une balise avec la valeur **production**, quelle que soit la clé de balise.

```
aws ec2 describe-instances \  
  --filters Name=tag-value,Values=production
```

Exemple Exemple : Décrire toutes les ressources EC2 avec la balise spécifiée

La commande suivante décrit toutes les ressources EC2 avec la balise **Stack=Test**.

```
aws ec2 describe-tags \  
  --filters Name=tag-key,Values=Stack
```

```
--filters Name=key,Values=Stack Name=value,Values=Test
```

Utiliser les identifications d'instance dans les métadonnées d'instance

Vous pouvez accéder aux identifications d'une instance à partir des métadonnées de l'instance. En accédant aux identifications à partir des métadonnées de l'instance, vous n'avez plus besoin d'utiliser le ou les appels d'API `DescribeInstances` ou `DescribeTags` pour récupérer les informations d'identification, ce qui réduit vos transactions d'API par seconde et permet à vos extractions d'identification de se mettre à l'échelle en fonction du nombre d'instances que vous contrôlez. En outre, les processus locaux exécutés sur une instance peuvent afficher les informations d'identification de l'instance directement à partir des métadonnées de l'instance.

Par défaut, les identifications ne sont pas disponibles à partir des métadonnées de l'instance. Vous devez explicitement autoriser l'accès. Vous pouvez autoriser l'accès au lancement de l'instance ou après le lancement sur une instance en cours d'exécution ou arrêtée. Vous pouvez également autoriser l'accès aux identifications en le spécifiant dans un modèle de lancement. Les instances lancées à l'aide du modèle permettent d'accéder aux identifications dans les métadonnées de l'instance.

Si vous ajoutez ou supprimez une balise d'instance, les métadonnées de l'instance sont mises à jour pendant que l'instance est exécutée, sans avoir besoin d'arrêter puis de démarrer l'instance.

Rubriques

- [Autoriser l'accès aux identifications dans les métadonnées d'instance](#)
- [Désactiver l'accès aux identifications dans les métadonnées d'instance](#)
- [Voir si l'accès aux balises dans les métadonnées d'instance est autorisé](#)
- [Extraire les identifications à partir des métadonnées d'instance](#)

Autoriser l'accès aux identifications dans les métadonnées d'instance

Par défaut, il n'y a pas d'accès aux balises d'instance dans les métadonnées de l'instance. Pour chaque instance, vous devez explicitement autoriser l'accès en utilisant l'une des méthodes suivantes.

Pour autoriser l'accès aux identifications dans les métadonnées d'instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez une instance, puis choisissez Actions, Instance settings (Paramètres de l'instance), Allow tags in instance metadata (Autoriser les identifications dans les métadonnées d'instance).
4. Pour autoriser l'accès aux identifications dans les métadonnées d'instance, cochez la case Allow (Autoriser).
5. Choisissez Enregistrer.

Pour autoriser l'accès aux identifications dans les métadonnées d'instance lors du lancement à l'aide de la AWS CLI

Utilisez la commande [run-instances](#) et définissez le paramètre InstanceMetadataTags sur enabled.

```
aws ec2 run-instances \  
  --image-id ami-0abcdef1234567890 \  
  --instance-type c3.large \  
  ... \  
  --metadata-options "InstanceMetadataTags=enabled"
```

Pour autoriser l'accès aux identifications dans les métadonnées d'instance sur une instance en cours d'exécution ou arrêtée à l'aide de la AWS CLI

Utilisez la commande [modify-instance-metadata-options](#) et définissez le paramètre `--instance-metadata-tags` sur enabled.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-123456789example \  
  --instance-metadata-tags enabled
```

Désactiver l'accès aux identifications dans les métadonnées d'instance

Pour désactiver l'accès aux identifications d'instance dans les métadonnées d'instance, utilisez l'une des méthodes suivantes. Il n'est pas nécessaire de désactiver l'accès aux identifications d'instance sur les métadonnées d'instance au lancement car il est désactivé par défaut.

Pour désactiver l'accès aux identifications dans les métadonnées d'instance à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez une instance, puis choisissez Actions, Instance settings (Paramètres de l'instance), Allow tags in instance metadata (Autoriser les identifications dans les métadonnées d'instance).
4. Pour désactiver l'accès aux identifications dans les métadonnées d'instance, décochez la case Allow (Autoriser).
5. Choisissez Enregistrer.

Pour désactiver l'accès aux balises dans les métadonnées de l'instance à l'aide du AWS CLI

Utilisez la commande [modify-instance-metadata-options](#) et définissez le paramètre `--instance-metadata-tags` sur `disabled`.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-123456789example \  
  --instance-metadata-tags disabled
```

Voir si l'accès aux balises dans les métadonnées d'instance est autorisé

Pour chaque instance, vous pouvez utiliser la console Amazon EC2 ou AWS CLI vérifier si l'accès aux balises d'instance à partir des métadonnées de l'instance est autorisé.

Pour voir si l'accès aux balises dans les métadonnées d'instance est autorisé à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances, puis sélectionnez l'instance.
3. Dans l'onglet Details (Détails), vérifiez le champ Allow tags in instance metadata (Autoriser les balises dans les métadonnées d'instance). Si la valeur est Enabled (Activé), les balises sont autorisées dans les métadonnées d'instance. Si la valeur est Disabled (Désactivé), les balises ne sont pas autorisées dans les métadonnées d'instance.

Pour savoir si l'accès aux balises dans les métadonnées de l'instance est autorisé à l'aide du AWS CLI

Utilisez la commande [describe-instances](#) et spécifiez l'ID de l'instance.

```
aws ec2 describe-instances \  
  --instance-ids i-1234567890abcdef0
```

L'exemple suivant de sortie est tronqué faute d'espace. Le paramètre "InstanceMetadataTags" indique si les balises sont autorisées dans les métadonnées d'instance. Si la valeur est `enabled`, les balises sont autorisées dans les métadonnées d'instance. Si la valeur est `disabled`, les balises ne sont pas autorisées dans les métadonnées d'instance.

```
{
  "Reservations": [
    {
      "Groups": [],
      "Instances": [
        {
          "AmiLaunchIndex": 0,
          "ImageId": "ami-0abcdef1234567890",
          "InstanceId": "i-1234567890abcdef0",
          ...
        }
      ]
    }
  ],
  "MetadataOptions": {
    "State": "applied",
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "disabled",
    "InstanceMetadataTags": "enabled"
  },
  ...
}
```

Extraire les identifications à partir des métadonnées d'instance

Si les identifications d'instance sont autorisées dans les métadonnées de l'instance, la catégorie `tags/instance` est accessible à partir des métadonnées de l'instance. Pour obtenir des exemples sur la façon d'extraire les identifications à partir des métadonnées de l'instance, consultez [Obtenir les identifications d'une instance](#).

Ajoutez des balises à une ressource à l'aide de CloudFormation

Avec les types de ressource Amazon EC2, vous spécifiez des balises à l'aide d'une propriété `Tags` ou `TagSpecifications`.

Les exemples suivants ajoutent la balise **Stack=Production** à [AWS::EC2::Instance](#) à l'aide de sa `Tags` propriété.

Exemple Exemple : Tags dans YAML

```
Tags:
- Key: "Stack"
  Value: "Production"
```

Exemple Exemple : Tags dans JSON

```
"Tags": [
  {
    "Key": "Stack",
    "Value": "Production"
  }
]
```

Les exemples suivants ajoutent la balise **Stack=Production** à [AWS::EC2::LaunchTemplate](#) [LaunchTemplateData](#) à l'aide de sa TagSpecifications propriété.

Exemple Exemple : TagSpecifications en YAML

```
TagSpecifications:
- ResourceType: "instance"
  Tags:
  - Key: "Stack"
    Value: "Production"
```

Exemple Exemple : TagSpecifications en JSON

```
"TagSpecifications": [
  {
    "ResourceType": "instance",
    "Tags": [
      {
        "Key": "Stack",
        "Value": "Production"
      }
    ]
  }
]
```

Quotas de service Amazon EC2

Amazon EC2 fournit différentes ressources que vous pouvez utiliser. Ces ressources incluent des images, des instances, des volumes et des instantanés (snapshot). Lorsque vous créez votre Compte AWS, nous définissons des quotas par défaut (également appelés limites) pour ces ressources par région. Par exemple, il existe un nombre maximal d'instances que vous pouvez lancer dans une région. Par exemple, si vous lancez une instance dans la région USA Ouest (Oregon), la demande ne doit pas faire en sorte que votre utilisation dépasse votre nombre maximal d'instances dans cette région.

La console Service Quotas est un emplacement central où vous pouvez consulter et gérer vos quotas de AWS services, et demander une augmentation des quotas pour la plupart des ressources que vous utilisez. Utilisez les informations de quota que nous fournissons pour gérer votre AWS infrastructure. Prévoyez de demander les augmentations de quota avant le moment où vous en aurez besoin.

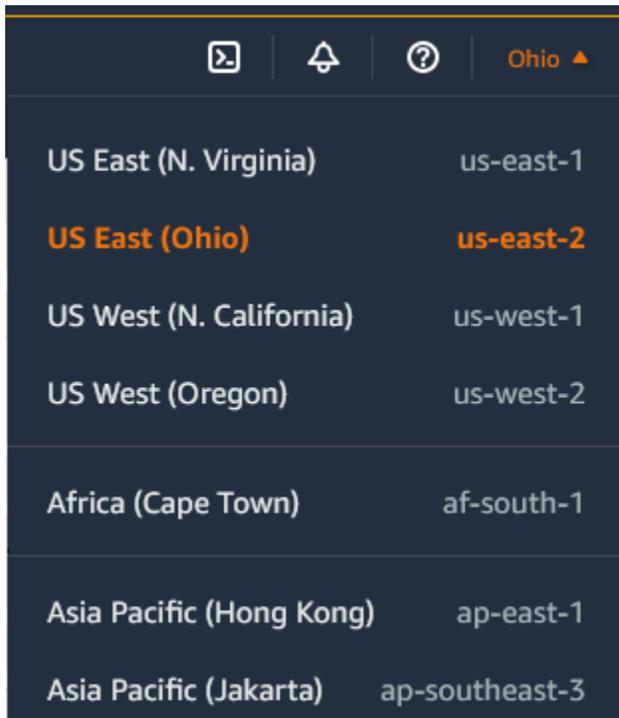
Pour plus d'informations, consultez les sections Points de [terminaison et quotas Amazon EC2](#) et [Points de terminaison et quotas Amazon EBS](#) dans le. Référence générale d'Amazon Web Services

Afficher vos quotas actuels

Vous pouvez afficher vos quotas pour chaque région à l'aide de la console Service Quotas.

Pour afficher vos quotas actuels à l'aide de la console Service Quotas

1. Ouvrez la console Service Quotas à l'adresse <https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/>.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez une région.



Region	Region ID
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Africa (Cape Town)	af-south-1
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Jakarta)	ap-southeast-3

3. Utilisez le champ de filtre pour filtrer la liste par nom de ressource. Par exemple, saisissez **On-Demand** pour connaître les quotas des instances à la demande.
4. Pour plus d'informations, choisissez le nom du quota afin d'ouvrir la page de détails du quota.

Demander une augmentation

Vous pouvez demander une augmentation de quota pour chaque région.

Pour demander une augmentation à l'aide de la console Service Quotas

1. Ouvrez la console Service Quotas à l'adresse <https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/>.
2. Dans la barre de navigation (en haut de l'écran), sélectionnez une région.
3. Utilisez le champ de filtre pour filtrer la liste par nom de ressource. Par exemple, saisissez **On-Demand** pour connaître les quotas des instances à la demande.
4. Si le quota est ajustable, sélectionnez-le, puis choisissez Demander une augmentation de quota.
5. Pour Modifier la valeur du quota, saisissez la nouvelle valeur du quota.
6. Choisissez Request (Demander).
7. Pour afficher les demandes en attente ou récemment résolues dans la console, choisissez Tableau de bord dans le volet de navigation. Pour les demandes en attente, choisissez l'état

de la demande pour ouvrir le reçu de la demande. L'état initial d'une demande est Pending (En attente). Une fois que le statut est passé au quota demandé, vous verrez le numéro de dossier avec AWS Support. Choisissez le numéro de dossier pour ouvrir le billet pour votre demande.

Pour plus d'informations, notamment sur la façon d'utiliser les AWS CLI SDK pour demander une augmentation de quota, consultez la section [Demander une augmentation de quota](#) dans le Guide de l'utilisateur du Service Quotas.

Restriction sur les e-mails envoyés à l'aide du port 25

Sur toutes les instances, Amazon EC2 limite le trafic sortant vers les adresses IP publiques sur le port 25 par défaut. Vous pouvez demander que cette restriction soit supprimée. Pour plus d'informations, consultez [Comment supprimer la restriction sur le port 25 de mon instance Amazon EC2 ou de ma fonction Lambda ?](#)

Note

Cette restriction ne s'applique pas au trafic sortant envoyé sur le port 25 aux :

- adresses IP dans le bloc d'adresse CIDR principal du VPC dans lequel l'interface réseau d'origine existe ;
- adresses IP dans les CIDR définis dans [RFC 1918](#), [RFC 6598](#) et [RFC 4193](#).

Résoudre les problèmes liés aux instances EC2

Les procédures et conseils suivants peuvent vous aider à résoudre les problèmes liés à vos instances Amazon EC2.

Table des matières

- [Problèmes courants avec les instances Windows](#)
- [Messages courants avec les instances Windows](#)
- [Résoudre les problèmes de lancement d'instance](#)
- [Résoudre les problèmes de connexion à votre instance Linux](#)
- [Résoudre les problèmes de connexion à votre instance Windows](#)
- [Réinitialisation d'un mot de passe administrateur Windows perdu ou expiré](#)
- [Résolution d'un problème d'instance inaccessible](#)
- [Résoudre les problèmes d'arrêt de votre instance](#)
- [Résoudre les problèmes de résiliation d'instance \(arrêt\)](#)
- [Résoudre les problèmes des instances Linux dont les vérifications d'état ont échoué](#)
- [Résoudre les problèmes liés au démarrage d'une instance Linux à partir d'un volume incorrect](#)
- [Résoudre les problèmes liés à Sysprep avec les instances Windows](#)
- [Utiliser EC2Rescue pour Linux](#)
- [Utiliser EC2Rescue for Windows Server](#)
- [Console série EC2 pour instances Amazon EC2](#)
- [Envoi d'une interruption de diagnostic \(utilisateurs avancés uniquement\)](#)

Problèmes courants avec les instances Windows

Voici des conseils de dépannage pour vous aider à résoudre les problèmes courants liés aux instances Windows Server EC2.

Problèmes

- [Les volumes EBS ne s'initialisent pas sur Windows Server 2016 et 2019](#)
- [Démarrer une instance Windows EC2 en mode de restauration des services d'annuaire \(DSRM\)](#)

- [L'instance perd la connectivité réseau ou les tâches programmées ne s'exécutent pas au moment prévu](#)
- [Impossible d'obtenir la sortie de la console](#)
- [Windows Server 2012 R2 non disponible sur le réseau](#)
- [Collision de signature de disque](#)

Les volumes EBS ne s'initialisent pas sur Windows Server 2016 et 2019

Les instances créées à partir des AMI (Amazon Machine Image) pour Windows Server 2016 et 2019 utilisent l'agent EC2Launch v1 pour un grand nombre de tâches de démarrage, notamment l'initialisation des volumes EBS. Par défaut, EC2Launch v1 n'initialise pas les volumes secondaires. Toutefois, vous pouvez configurer EC2Launch v1 pour initialiser les disques automatiquement, comme suit.

Mapper les lettres de lecteur avec les volumes

1. Connectez-vous à l'instance que vous voulez configurer et ouvrez le fichier `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` dans un éditeur de texte.
2. Spécifiez les paramètres du volume, comme suit :

```
{
  "driveLetterMapping": [
    {
      "volumeName": "sample volume",
      "driveLetter": "H"
    }
  ]
}
```

3. Enregistrez les modifications, puis fermez le fichier.
4. Ouvrez Windows PowerShell et utilisez la commande suivante pour exécuter le script EC2Launch v1 qui initialise les disques :

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Pour initialiser les disques chaque fois que l'instance démarre, ajoutez l'indicateur `-Schedule` comme suit :

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

L'agent EC2Launch v1 peut exécuter des scripts d'initialisation d'instance tels que `initializeDisks.ps1` en parallèle avec le script `InitializeInstance.ps1`. Si le script `InitializeInstance.ps1` redémarre l'instance, il peut interrompre d'autres tâches planifiées qui s'exécutent au démarrage de l'instance. Pour éviter tout conflit potentiel, nous vous recommandons d'ajouter de la logique à votre script `initializeDisks.ps1` pour vous assurer que l'initialisation de l'instance est terminée en premier.

Note

Si le script EC2Launch n'initialise pas les volumes, assurez-vous que les volumes sont en ligne. Si les volumes sont hors ligne, exécutez la commande suivante pour mettre tous les disques en ligne.

```
PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
$False
```

Démarrer une instance Windows EC2 en mode de restauration des services d'annuaire (DSRM)

Si une instance s'exécutant sur Microsoft Active Directory fait l'objet d'une défaillance système ou rencontre d'autres problèmes majeurs, vous pouvez la dépanner en la démarrant dans une version spéciale du mode sans échec Safe Mode appelé Mode de restauration des services d'annuaire (DSRM). Le mode DSRM vous permet de réparer ou de récupérer Active Directory.

Prise en charge du pilote de DSRM

La méthode avec laquelle vous activez le mode DSRM et démarrez dans l'instance dépend des pilotes que l'instance exécute. Dans la console EC2, vous pouvez afficher les détails de la version du pilote d'une instance dans le journal système. Le tableau suivant montre quels sont les pilotes pris en charge pour DSRM.

Versions des pilotes	Mode DSRM pris en charge ?	Étapes suivantes
PV Citrix 5.9	Non	Restaurez l'instance à partir d'une sauvegarde. Vous ne pouvez pas activer le mode DSRM.
AWS PV 7.2.0	Non	Si DSRM n'est pas pris en charge pour ce pilote, vous pouvez toujours détacher le volume racine de l'instance, créer un instantané ou une AMI du volume et l'attacher à une autre instance dans la même zone de disponibilité en tant que volume secondaire. Vous pouvez ensuite activer DSRM (comme décrit dans cette section).
AWS PV 7.2.2 et versions ultérieures	Oui	Détachez le volume racine, attachez-le à une autre instance, puis activez le mode DSRM (comme décrit dans cette section).
Mise en réseau améliorée	Oui	Détachez le volume racine, attachez-le à une autre instance, puis activez le mode DSRM (comme décrit dans cette section).

Pour plus d'informations sur la façon d'activer la mise en réseau améliorée, consultez [the section called “Elastic Network Adapter \(ENA\)”](#). Pour plus d'informations sur la mise à niveau des pilotes AWS PV, voir [Mettre à niveau les pilotes PV sur les instances Windows](#).

Configurer une instance à démarrer dans le mode DSRM

Les instances Windows EC2 n'ont pas de connectivité réseau tant que le système d'exploitation ne s'exécute pas. C'est pourquoi vous ne pouvez pas appuyer sur la touche F8 de votre clavier pour sélectionner une option de démarrage. Vous devez utiliser l'une des procédures suivantes pour démarrer une instance Windows Server EC2 dans le mode DSRM.

Si vous craignez qu'Active Directory ait été corrompu et que l'instance soit toujours en cours d'exécution, vous pouvez configurer l'instance pour démarrer dans le mode DSRM à l'aide de la boîte de dialogue Configuration du système ou l'invite de commande.

Pour démarrer une instance en ligne dans le mode DSRM à l'aide de la boîte de dialogue Configuration du système

1. Dans la boîte de dialogue Exécuter, tapez `msconfig` et appuyez sur Entrée.
2. Choisissez l'onglet Démarrage.
3. Sous Options de démarrage, choisissez Démarrage sécurisé.
4. Choisissez Réparer Active Directory, puis OK. Le système vous invite à redémarrer le serveur.

Pour démarrer une instance en ligne dans le mode DSRM à l'aide de la ligne de commande

A partir d'une fenêtre d'invite de commande, exécutez la commande suivante :

```
bcdedit /set safeboot dsrepair
```

Si une instance est hors ligne et inaccessible, vous devez détacher le volume racine et l'attacher à une autre instance pour activer le mode DSRM.

Pour démarrer une instance hors ligne dans le mode DSRM

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Recherchez et sélectionnez l'instance affectée. Choisissez État de l'instance, Arrêter l'instance.
4. Choisissez Lancer les instances et créez une instance temporaire dans la même zone de disponibilité que l'instance affectée. Choisissez un type d'instance qui utilise une autre version de Windows. Par exemple, si votre instance est Windows Server 2016, choisissez une instance Windows Server 2019.

Important

Si vous ne créez pas l'instance dans la même zone de disponibilité que l'instance affectée, vous ne pourrez pas attacher le volume racine de celle-ci à la nouvelle instance.

5. Dans le panneau de navigation, choisissez Volumes.
6. Recherchez le volume racine de l'instance affectée. [Détachez](#) le volume et [attachez](#)-le à l'instance temporaire que vous avez créée précédemment. Attachez-le avec le nom du périphérique par défaut (`xvdf`).

7. Utilisez les services Bureau à distance pour vous connecter à l'instance temporaire, puis utilisez l'utilitaire Gestion des disques pour [rendre le volume disponible](#).
8. Ouvrez une invite de commande et exécutez la commande suivante. Remplacez D par la lettre de lecteur réelle du volume secondaire que vous venez d'attacher :

```
bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
```

9. Dans l'utilitaire Gestion des disques, choisissez le lecteur que vous avez attaché précédemment, ouvrez le menu contextuel (clic droit) et choisissez Hors connexion.
10. Dans la console Amazon EC2, détachez le volume affecté de l'instance temporaire et rattachez-le à votre instance originale avec le nom de périphérique /dev/sda1. Vous devez spécifier ce nom de périphérique pour désigner le volume en tant que volume racine.
11. [Démarez](#) l'instance.
12. Une fois que l'instance réussit les vérifications de l'état dans la console EC2, connectez-vous à l'instance à l'aide des services Bureau à distance et vérifiez qu'elle démarre dans le mode DSRM.
13. (Facultatif) Supprimez ou arrêtez l'instance temporaire que vous avez créée au cours de cette procédure.

L'instance perd la connectivité réseau ou les tâches programmées ne s'exécutent pas au moment prévu

Si vous redémarrez votre instance et qu'elle perd sa connectivité réseau, il est possible que l'instance ne soit pas à l'heure.

Par défaut, les instances Windows utilisent l'heure universelle coordonnée (UTC). Si vous définissez l'heure de votre instance sur un autre fuseau horaire et que vous la redémarrez, l'heure se décale et l'instance perd temporairement son adresse IP. L'instance finit par rétablir sa connectivité réseau, mais cela peut prendre plusieurs heures. Le délai nécessaire pour que l'instance rétablisse sa connectivité réseau dépend de la différence entre l'heure universelle coordonnée (UTC) et l'autre fuseau horaire.

Ce problème peut également entraîner l'absence d'exécution de tâches planifiées au moment prévu. Dans ce cas, les tâches planifiées ne s'exécutent pas au moment prévu, car l'heure de l'instance est incorrecte.

Pour utiliser un fuseau horaire autre que UTC de manière persistante, vous devez définir la clé de `RealTimeIsUniversal`. Sans cette clé, une instance utilise l'heure universelle coordonnée (UTC) après avoir redémarré.

Pour résoudre les problèmes d'heure qui entraînent une perte de la connectivité réseau

1. Vérifiez que vous exécutez les pilotes PV recommandés. Pour plus d'informations, consultez [the section called "Mettre à niveau les pilotes PV"](#).
2. Vérifiez que la clé de registre suivante existe et qu'elle est définie sur 1 :
`HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControl Set \ Control \ Information \ TimeZone RealTime IsUniversal`

Impossible d'obtenir la sortie de la console

Pour les instances Windows, la sortie de la console de l'instance affiche la sortie des tâches exécutées à l'aide du processus d'amorçage Windows. Si Windows démarre correctement, le dernier message enregistré est `Windows is Ready to use`. Vous pouvez également afficher les messages du journal des événements dans la console, mais cette fonctionnalité peut ne pas être activée par défaut en fonction de votre version de Windows. Pour plus d'informations, consultez [the section called "Configuration des agents de lancement Windows"](#).

Pour obtenir la sortie de la console de votre instance à l'aide de la console Amazon EC2, sélectionnez l'instance, puis Actions, Surveiller et dépanner et Obtenir le journal système. Pour obtenir le résultat de la console à l'aide de la ligne de commande, utilisez l'une des commandes suivantes : [get-console-output \(AWS CLI\)](#) ou [\(\). Get-EC2ConsoleOutput](#) AWS Tools for Windows PowerShell

Pour les instances exécutant Windows Server 2012 R2 et versions antérieures, si la sortie de la console est vide, cela peut indiquer un problème avec le service EC2Config, comme un fichier de configuration mal configuré, ou que Windows a échoué à démarrer correctement. Pour corriger ce problème, téléchargez et installez la version la plus récente d'EC2Config. Pour plus d'informations, consultez [the section called "Installer EC2Config"](#).

Windows Server 2012 R2 non disponible sur le réseau

Pour plus d'informations sur le dépannage d'une instance Windows Server 2012 R2 qui n'est pas disponible sur le réseau, voir [Windows Server 2012 R2 perd la connectivité réseau et de stockage après le redémarrage d'une instance](#).

Collision de signature de disque

Vous pouvez rechercher et résoudre les collisions de signature de disque à l'aide de [EC2Rescue for Windows Server](#). Vous pouvez également résoudre manuellement les problèmes de signature de disque en effectuant les opérations suivantes :

Warning

La procédure suivante décrit comment modifier le Registre Windows à l'aide de l'Éditeur de Registre. Si vous n'êtes pas familier avec le Registre Windows ou comment apporter des modifications en toute sécurité à l'aide de l'Éditeur de Registre, consultez [Configurer le registre](#).

1. Ouvrez une invite de commande, saisissez regedit.exe, puis appuyez sur Entrée.
2. Dans Editeur de registre, choisissez HKEY_LOCAL_MACHINE dans le menu contextuel (clic droit), puis choisissez Rechercher.
3. Cliquez sur Windows Boot Manager, puis choisissez Rechercher suivant.
4. Choisissez la clé nommée 11000001. Cette clé est apparentée à la clé que vous avez trouvée à l'étape précédente.
5. Dans le volet droit, choisissez Element, puis Modifier à partir du menu contextuel (clic droit).
6. Localisez la signature du disque de quatre octets au décalage 0x38 dans les données. Il s'agit de la signature BCD (Boot Configuration Database). Inversez les octets pour créer la signature du disque et l'écrire. Par exemple, la signature de disque représentée par les données suivantes est E9EB3AA5 :

```
...  
0030  00 00 00 00 01 00 00 00  
0038  A5 3A EB E9 00 00 00 00  
0040  00 00 00 00 00 00 00 00  
...
```

7. Dans une fenêtre d'invite de commandes, exécutez la commande suivante pour démarrer Microsoft DiskPart.

```
diskpart
```

8. Exécutez la `select disk` DiskPart commande et spécifiez le numéro de disque du volume concerné par la collision de signature de disque.

 Tip

Pour vérifier le numéro de disque du volume présentant la collision de signature de disque, utilisez l'utilitaire Gestion des disques. Ouvrez une invite de commande, saisissez `compmgmt.msc`, puis appuyez sur Entrée. Dans le volet de navigation de gauche, double-cliquez sur Gestion des disques. Dans l'utilitaire Gestion des disques, vérifiez le numéro de disque du volume présentant la collision de signature de disque.

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

9. Exécutez la DiskPart commande suivante pour obtenir la signature du disque.

```
DISKPART> uniqueid disk
Disk ID: 0C764FA8
```

10. Si la signature de disque affichée à l'étape précédente ne correspond pas à la signature de disque que vous avez notée précédemment, utilisez la DiskPart commande suivante pour modifier la signature de disque afin qu'elle corresponde :

```
DISKPART> uniqueid disk id=E9EB3AA5
```

Messages courants avec les instances Windows

Cette section inclut des conseils pour vous aider à résoudre les problèmes sur la base de messages courants.

Messages

- [« Le mot de passe n'est pas disponible »](#)
- [« Mot de passe pas encore disponible »](#)
- [« Récupération du mot de passe Windows impossible »](#)
- [« En attente du service de métadonnées »](#)

- [« L'activation de Windows est impossible »](#)
- [« Windows n'est pas authentique \(0x80070005\) »](#)
- [« Aucun serveur de licences Terminal Server n'est disponible pour fournir une licence »](#)
- [« Certains paramètres sont gérés par votre organisation »](#)

« Le mot de passe n'est pas disponible »

Pour vous connecter à une instance Windows à l'aide des services Bureau à distance, vous devez spécifier un compte et un mot de passe. Les comptes et mots de passe fournis sont basés sur l'AMI que vous avez utilisée pour lancer l'instance. Vous pouvez récupérer le mot de passe généré automatiquement pour le compte d'administrateur ou utiliser le compte et le mot de passe utilisés dans l'instance originale à partir de laquelle l'AMI a été créée.

Vous pouvez générer un mot de passe pour le compte administrateur des instances lancées à l'aide d'une AMI Windows personnalisée. Pour générer le mot de passe, vous devrez configurer certains paramètres du système d'exploitation avant la création de l'AMI. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).

Si votre instance Windows n'est pas configurée pour générer un mot de passe aléatoire, vous recevez le message suivant lorsque vous extrayez le mot de passe généré automatiquement à l'aide de la console :

```
Password is not available.  
The instance was launched from a custom AMI, or the default password has changed. A  
password cannot be retrieved for this instance. If you have forgotten your password,  
you can  
reset it using the Amazon EC2 configuration service. For more information, see  
Passwords for a  
Windows Server instance.
```

Recherchez l'instance dans la sortie de la console pour voir si l'AMI que vous avez utilisée pour lancer l'instance a été créée avec la génération de mot de passe désactivée. Si la génération de mot de passe est désactivée, la sortie de la console contient ce qui suit :

```
Ec2SetPassword: Disabled
```

Si la génération de mot de passe est désactivée et que vous avez oublié le mot de passe de l'instance originale, vous pouvez réinitialiser le mot de passe de cette instance. Pour plus d'informations, consultez [Réinitialisation d'un mot de passe administrateur Windows perdu ou expiré](#).

« Mot de passe pas encore disponible »

Pour vous connecter à une instance Windows à l'aide des services Bureau à distance, vous devez spécifier un compte et un mot de passe. Les comptes et mots de passe fournis sont basés sur l'AMI que vous avez utilisée pour lancer l'instance. Vous pouvez récupérer le mot de passe généré automatiquement pour le compte d'administrateur ou utiliser le compte et le mot de passe utilisés dans l'instance originale à partir de laquelle l'AMI a été créée.

Votre mot de passe devrait être disponible d'ici quelques minutes. Si le mot de passe n'est pas disponible, vous recevrez le message suivant lorsque vous extrayez le mot de passe généré automatiquement à l'aide de la console :

```
Password not available yet.  
Please wait at least 4 minutes after launching an instance before trying to retrieve  
the  
auto-generated password.
```

Si cela fait plus de quatre minutes et que vous ne pouvez toujours pas obtenir le mot de passe, il est possible que l'agent de lancement de votre instance ne soit pas configuré pour générer un mot de passe. Pour cela, vérifiez si la sortie de la console est vide. Pour plus d'informations, consultez [Impossible d'obtenir la sortie de la console](#).

Vérifiez également que `ec2:GetPasswordData` action est autorisée sur le compte AWS Identity and Access Management (IAM) utilisé pour accéder au portail de gestion. Pour plus d'informations sur les autorisations IAM, consultez [Qu'est-ce qu'IAM ?](#)

« Récupération du mot de passe Windows impossible »

Pour récupérer le mot de passe généré automatiquement pour le compte d'administrateur, vous devez utiliser la clé privée de la paire de clés que vous avez spécifiée lors du lancement de l'instance. Si vous n'avez pas spécifié de paire de clés existante au lancement de l'instance, vous recevez le message suivant.

```
Cannot retrieve Windows password
```

Vous pouvez mettre cette instance hors service et lancer une nouvelle instance à l'aide de la même AMI, en veillant à spécifier une paire de clés.

« En attente du service de métadonnées »

Une instance Windows doit obtenir des informations auprès des métadonnées de son instance avant qu'elle puisse s'activer. Par défaut, le paramètre `WaitForMetadataAvailable` vérifie que le service EC2Config attend que les métadonnées de l'instance soient accessibles avant de poursuivre le processus de démarrage. Pour plus d'informations, consultez [Utiliser des métadonnées d'instance](#).

Si l'instance échoue au test d'accessibilité de l'instance, essayez la solution suivante pour résoudre le problème.

- Vérifiez le bloc d'adresse CIDR de votre VPC. Une instance Windows ne peut pas démarrer correctement si elle est lancée dans un VPC ayant une plage d'adresses IP comprise entre 224.0.0.0 et 255.255.255.255 (plages d'adresses IP de classe D et de classe E). Ces plages d'adresses IP sont réservées et ne doivent pas être attribuées aux périphériques hôtes. Nous vous conseillons de créer un VPC avec un bloc d'adresse CIDR des plages d'adresses IP privées (non publiquement routables), comme spécifié dans la norme [RFC 1918](#).
- Il est possible que le système ait été configuré avec une adresse IP statique. Essayez de [créer une interface réseau](#) et de [l'attacher à l'instance](#).
- Pour activer DHCP sur une instance Windows à laquelle vous ne parvenez pas à vous connecter
 1. Arrêtez l'instance affectée et détachez son volume racine.
 2. Lancez une instance temporaire dans la même zone de disponibilité que l'instance affectée.

Warning

Si votre instance temporaire est basée sur la même AMI que l'instance d'origine, vous devez effectuer des étapes supplémentaires. Dans le cas contraire, vous ne serez pas en mesure de démarrer l'instance d'origine après la restauration de son volume racine en raison d'une collision de signature de disque. Sinon, sélectionnez une autre AMI pour l'instance temporaire. Par exemple, si l'instance d'origine utilise l'AMI AWS Windows pour Windows Server 2016, lancez l'instance temporaire à l'aide de l'AMI AWS Windows pour Windows Server 2019.

3. Attachez le volume racine de l'instance affectée à cette instance temporaire. Connectez-vous à l'instance temporaire, ouvrez l'utilitaire Gestion des disques et mettez le lecteur en ligne.

4. Dans l'instance temporaire, ouvrez Regedit et sélectionnez HKEY_LOCAL_MACHINE. Dans le menu File (Fichier), choisissez Load Hive (Charger Hive). Sélectionnez le lecteur, ouvrez le fichier `Windows\System32\config\SYSTEM` et spécifiez un nom de clé lorsque vous y êtes invité (vous pouvez utiliser n'importe quel nom).
5. Sélectionnez la clé que vous venez de charger et naviguez jusqu'à `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Chaque interface réseau est répertoriée par un GUID. Sélectionnez l'interface réseau correcte. Si DHCP est désactivé et qu'une adresse IP statique est attribuée, `EnableDHCP` est défini sur 0. Pour activer DHCP, définissez `EnableDHCP` sur 1 et supprimez les clés suivantes si elles existent : `NameServer`, `SubnetMask`, `IPAddress` et `DefaultGateway`. Sélectionnez à nouveau la clé, puis dans le menu File (Fichier), sélectionnez Unload Hive (Décharger Hive).

 Note

Si vous avez plusieurs interfaces réseau, vous devrez identifier l'interface appropriée pour activer DHCP. Pour identifier l'interface réseau appropriée, consultez les valeurs de clé `NameServer`, `SubnetMask`, `IPAddress` et `DefaultGateway`. Ces valeurs affichent la configuration statique de l'instance précédente.

6. (Facultatif) Si DHCP est déjà activé, il est possible que vous ne disposiez pas d'une route vers le service de métadonnées. La mise à niveau d'EC2Config peut résoudre ce problème.
 - a. [Téléchargez](#) et installez la dernière versions du service EC2Config. Pour en savoir plus sur l'installation de ce service, consultez [the section called "Installer EC2Config"](#).
 - b. Extrayez les fichiers du fichier .zip dans le répertoire Temp du lecteur que vous avez attaché.
 - c. Ouvrez Regedit et sélectionnez HKEY_LOCAL_MACHINE. Dans le menu File (Fichier), choisissez Load Hive (Charger Hive). Sélectionnez le lecteur, ouvrez le fichier `Windows\System32\config\SOFTWARE` et spécifiez un nom de clé lorsque vous y êtes invité (vous pouvez utiliser n'importe quel nom).
 - d. Sélectionnez la clé que vous venez de charger et naviguez jusqu'à `Microsoft\Windows\CurrentVersion`. Sélectionnez la clé `RunOnce`. (Si elle n'existe pas, cliquez avec le bouton droit sur `CurrentVersion`, pointez la souris vers Nouveau, sélectionnez Clé et nommez la clé `RunOnce`.) Cliquez avec le bouton droit, pointez la souris vers Nouveau et sélectionnez Valeur de chaîne. Entrez le nom `Ec2Install` et les données `C:\Temp\Ec2Install.exe -q`.

- e. Sélectionnez à nouveau la clé, puis dans le menu File (Fichier), sélectionnez Unload Hive (Décharger Hive).
7. (Facultatif) Si votre instance temporaire est basée sur la même AMI que l'instance d'origine, vous devez effectuer les étapes suivantes. Dans le cas contraire, vous ne serez pas en mesure de démarrer l'instance d'origine après la restauration de son volume racine en raison d'une collision de signature de disque.

⚠ Warning

La procédure suivante décrit comment modifier le Registre Windows à l'aide de l'Éditeur de Registre. Si vous n'êtes pas familier avec le Registre Windows ou comment apporter des modifications en toute sécurité à l'aide de l'Éditeur de Registre, consultez [Configurer le registre](#).

- a. Ouvrez une invite de commande, saisissez regedit.exe, puis appuyez sur Entrée.
- b. Dans Editeur de registre, choisissez HKEY_LOCAL_MACHINE dans le menu contextuel (clic droit), puis choisissez Rechercher.
- c. Cliquez sur Windows Boot Manager, puis choisissez Rechercher suivant.
- d. Choisissez la clé nommée 11000001. Cette clé est apparentée à la clé que vous avez trouvée à l'étape précédente.
- e. Dans le volet droit, choisissez Element, puis Modifier à partir du menu contextuel (clic droit).
- f. Localisez la signature du disque de quatre octets au décalage 0x38 dans les données. Inversez les octets pour créer la signature du disque et l'écrire. Par exemple, la signature de disque représentée par les données suivantes est E9EB3AA5 :

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

- g. Dans une fenêtre d'invite de commandes, exécutez la commande suivante pour démarrer Microsoft DiskPart.

```
diskpart
```

- h. Exécutez la DiskPart commande suivante pour sélectionner le volume. (Vous pouvez vérifier que le numéro de disque est 1 à l'aide de l'utilitaire Gestion des disques.

```
DISKPART> select disk 1  
  
Disk 1 is now the selected disk.
```

- i. Exécutez la DiskPart commande suivante pour obtenir la signature du disque.

```
DISKPART> uniqueid disk  
  
Disk ID: 0C764FA8
```

- j. Si la signature de disque affichée à l'étape précédente ne correspond pas à la signature de disque de BCD que vous avez notée plus tôt, utilisez la DiskPart commande suivante pour modifier la signature de disque afin qu'elle corresponde :

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. À l'aide de l'utilitaire Gestion des disques, déconnectez le lecteur.

Note

Le lecteur est automatiquement hors ligne si l'instance temporaire exécute le même système d'exploitation que l'instance concernée. Vous n'aurez donc pas besoin de le mettre hors ligne manuellement.

9. Détachez le volume de l'instance temporaire. Vous pouvez mettre l'instance temporaire hors service si vous n'en avez plus besoin.
10. Restaurez le volume racine de l'instance affectée en attachant le volume en tant que /dev/sda1.
11. Démarrez l'instance concernée.

Si vous êtes connecté à l'instance, ouvrez un navigateur Internet dans l'instance et entrez l'URL suivante pour le serveur de métadonnées :

```
http://169.254.169.254/latest/meta-data/
```

Si vous ne pouvez pas contacter le serveur de métadonnées, essayez la solution suivante pour résoudre le problème :

- [Téléchargez](#) et installez la dernière versions du service EC2Config. Pour en savoir plus sur l'installation de ce service, consultez [the section called "Installer EC2Config"](#).
- Vérifiez si l'instance Windows exécute des pilotes RedHat PV. Si c'est le cas, mettez à jour les pilotes PV Citrix. Pour plus d'informations, consultez [the section called "Mettre à niveau les pilotes PV"](#).
- Vérifiez que les paramètres du pare-feu, de l'IPSec et du proxy ne bloquent pas le trafic sortant vers le service de métadonnées (169.254.169.254) ou les serveurs AWS KMS (les adresses sont spécifiées dans les éléments TargetKMSServer de C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml).
- Vérifiez que vous disposez d'une route vers le service de métadonnées (169.254.169.254) à l'aide de la commande suivante.

```
route print
```

- Vérifiez les problèmes de réseau susceptibles d'affecter la zone de disponibilité de votre instance. Accédez à <http://status.aws.amazon.com/>.

« L'activation de Windows est impossible »

Les instances Windows utilisent l' AWS KMS activation Windows. Vous pouvez recevoir ce message :A problem occurred when Windows tried to activate. Error Code 0xC004F074, si votre instance ne parvient pas à atteindre le AWS KMS serveur. Windows doit être activé tous les 180 jours. EC2Config tente de contacter le AWS KMS serveur avant l'expiration de la période d'activation pour s'assurer que Windows reste activé.

Si vous rencontrez un problème d'activation Windows, utilisez la procédure suivante pour le résoudre.

Pour EC2Config (AMI Windows Server 2012 R2 et antérieures)

1. [Téléchargez](#) et installez la dernière versions du service EC2Config. Pour en savoir plus sur l'installation de ce service, consultez [the section called "Installer EC2Config"](#).

2. Connectez-vous à l'instance et ouvrez le fichier suivant : `C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml`.
3. Localisez le `WindowsActivate` plugin Ec2 dans le `config.xml` fichier. Remplacez l'état par `Activé`, puis enregistrez vos modifications.
4. Dans le composant logiciel enfichable `Windows Services`, redémarrez le service `EC2Config` ou l'instance.

Si cette procédure ne résout pas le problème d'activation, suivez ces étapes supplémentaires.

1. Définissez l' AWS KMS objectif : `C:\> slmgr.vbs /skms 169.254.169.250:1688`
2. Activez Windows : `C:\> slmgr.vbs /ato`

Pour `EC2Launch` (AMI Windows Server 2016 et ultérieures)

1. À partir d'une PowerShell invite indiquant les droits d'administration, importez le module `EC2Launch` :

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psd1"
```

2. Appelez la fonction `Add-Routes` pour voir la liste des nouvelles routes :

```
PS C:\> Add-Routes
```

3. Appelez la `ActivationSettings` fonction `Set-` :

```
PS C:\> Set-Activationsettings
```

4. Ensuite, exécutez le script suivant pour activer Windows :

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Pour `EC2Config` et `EC2Launch`, si vous continuez à recevoir une erreur d'activation, vérifiez les informations ci-dessous.

- Vérifiez que vous disposez de routes vers les AWS KMS serveurs. Ouvrez `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` et recherchez les

éléments TargetKMS Server. Exécutez la commande suivante et vérifiez si les adresses de ces AWS KMS serveurs sont répertoriées.

```
route print
```

- Vérifiez que la clé AWS KMS client est définie. Exécutez la commande suivante et consultez la sortie.

```
C:\Windows\System32\slmgr.vbs /dlv
```

Si le résultat contient le message d'erreur : clé de produit introuvable, la clé AWS KMS client n'est pas définie. Si la clé AWS KMS client n'est pas définie, recherchez-la comme décrit dans cet article de Microsoft : [Clés de configuration du AWS KMS client](#), puis exécutez la commande suivante pour définir la clé AWS KMS client.

```
C:\Windows\System32\slmgr.vbs /ipk client_key
```

- Vérifiez que le système dispose de l'heure et du fuseau horaires adéquats. Si vous utilisez un fuseau horaire autre que UTC, ajoutez la clé de registre suivante et définissez-la 1 pour vous assurer que l'heure est correcte : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal
- Si le pare-feu Windows est activé, désactivez-le temporairement à l'aide de la commande suivante.

```
netsh advfirewall set allprofiles state off
```

« Windows n'est pas authentique (0x80070005) »

Les instances Windows utilisent l' AWS KMS activation Windows. Si une instance ne parvient pas à terminer le processus d'activation, elle signale que la copie de Windows n'est pas authentique.

Essayez les suggestions de la section [« L'activation de Windows est impossible »](#).

« Aucun serveur de licences Terminal Server n'est disponible pour fournir une licence »

Par défaut, la licence Windows Server autorise deux utilisateurs simultanés via les services Bureau à distance. Si vous devez fournir à plus de deux utilisateurs un accès simultané à votre instance

Windows via Bureau à distance, vous pouvez acheter une licence d'accès client (CAL) des services Bureau à distance et installer l'hôte de la session des services Bureau à distance et les rôles du Serveur du Gestionnaire de licences des services Bureau à distance.

Vérifiez les problèmes suivants :

- Vous avez dépassé le nombre maximal de sessions RDP simultanées.
- Vous avez installé le rôle des services Bureau à distance Windows.
- Le Gestionnaire de licences a expiré. Le cas échéant, vous ne pouvez pas vous connecter à votre instance Windows en tant qu'utilisateur. Vous pouvez essayer l'une des actions suivantes :
 - Connectez-vous à l'instance à partir de la ligne de commande à l'aide du paramètre `/admin`, par exemple :

```
mstsc /v:instance /admin
```

Pour plus d'informations, consultez l'article Microsoft suivant : [Access Remote Desktop Via Command Line](#).

- Arrêtez l'instance, détachez ses volumes Amazon EBS et attachez-les à une autre instance dans la même zone de disponibilité pour récupérer vos données.

« Certains paramètres sont gérés par votre organisation »

Les instances lancées à partir des dernières AMI Windows Server peuvent afficher un message contextuel Windows Update avec la mention « Certains paramètres sont gérés par votre organisation ». Ce message apparaît en réponse à des changements dans Windows Server et n'affecte pas le comportement de Windows Update, ni votre capacité à gérer les paramètres de mise à jour.

Pour supprimer l'avertissement

1. Ouvrez `gpedit.msc` et accédez à Configuration ordinateur, Modèles d'administration, Composants Windows, Mises à jour Windows. Modifiez Configurer la mise à jour automatique et définissez la valeur activé.
2. Dans une invite de commandes, mettez à jour la politique de groupe avec `gpupdate /force`.
3. Fermez et rouvrez les Paramètres de Windows Update. Vous verrez le message ci-dessus indiquant que vos paramètres sont gérés par votre organisation, suivi par « Nous téléchargerons automatiquement les mises à jour, sauf si vous disposez d'une connexion limitée (où des frais

s'appliquent). Dans ce cas, nous ne téléchargerons automatiquement que les mises à jour nécessaires au bon fonctionnement de Windows. »

4. Revenez à `gpedit.msc` et redéfinissez la stratégie de groupe sur la valeur non configuré. Exécutez à nouveau `gpupdate /force`.
5. Fermez l'invite de commande et patientez quelques minutes.
6. Rouvrez les Paramètres de Windows Update. Le message « Certains paramètres sont gérés par votre organisation. » ne doit pas s'afficher.

Résoudre les problèmes de lancement d'instance

Le problème suivant vous empêche de lancer une instance.

Problèmes de lancement

- [Nom de périphérique non valide](#)
- [Dépassement de la limite d'instance](#)
- [Capacité d'instance insuffisante](#)
- [La configuration demandée n'est actuellement pas prise en charge. Consultez la documentation pour voir les configurations prises en charge.](#)
- [Mise hors service immédiate de l'instance](#)
- [Autorisations insuffisantes](#)
- [Utilisation élevée du processeur peu après le démarrage de Windows \(instances Windows uniquement\)](#)

Nom de périphérique non valide

Description

Vous obtenez l'erreur `Invalid device name` *device_name* lorsque vous essayez de lancer une nouvelle instance.

Cause

Si vous obtenez cette erreur lorsque vous essayez de lancer une instance, le nom de périphérique spécifié pour un ou plusieurs volumes dans la demande comporte un nom de périphérique non valide. Les causes possibles incluent :

- Le nom de périphérique est peut-être déjà utilisé par l'AMI sélectionnée.
- Le nom de périphérique peut être réservé aux volumes racine.
- Le nom de périphérique peut être utilisé pour un autre volume dans la demande.
- Le nom de périphérique peut ne pas être valide pour le système d'exploitation.

Solution

Pour résoudre le problème :

- Assurez-vous que le nom de périphérique n'est pas utilisé dans l'AMI que vous avez sélectionnée. Exécutez la commande suivante pour afficher les noms de périphériques utilisés par l'AMI.

```
aws ec2 describe-images --image-id ami_id --query  
'Images[*].BlockDeviceMappings[].DeviceName '
```

- Assurez-vous que vous n'utilisez pas un nom de périphérique qui est réservé aux volumes racine. Pour plus d'informations, consultez [Noms d'appareil disponibles](#).
- Assurez-vous que chaque volume spécifié dans votre demande possède un nom de périphérique unique.
- Assurez-vous que les noms de périphériques que vous avez spécifiés sont au format correct. Pour plus d'informations, consultez [Noms d'appareil disponibles](#).

Dépassement de la limite d'instance

Description

Vous obtenez l'erreur `InstanceLimitExceeded` lorsque vous essayez de lancer une nouvelle instance ou de redémarrer une instance arrêtée.

Cause

Si vous obtenez une erreur `InstanceLimitExceeded` lorsque vous essayez de lancer une nouvelle instance ou de redémarrer une instance arrêté, vous avez atteint la limite du nombre d'instances que vous pouvez lancer dans une région. Lorsque vous créez votre AWS compte, nous fixons des limites par défaut quant au nombre d'instances que vous pouvez exécuter par région.

Solution

Vous pouvez demander une augmentation de la limite d'instance par région. Pour de plus amples informations, veuillez consulter [Quotas de service Amazon EC2](#).

Capacité d'instance insuffisante

Description

Vous obtenez l'erreur `InsufficientInstanceCapacity` lorsque vous essayez de lancer une nouvelle instance ou de redémarrer une instance arrêtée.

Cause

Si vous obtenez cette erreur lorsque vous essayez de lancer une instance ou de redémarrer une instance arrêtée, AWS n'a actuellement pas assez de capacité à la demande disponible pour répondre à votre demande.

Solution

Pour résoudre ce problème, essayez ce qui suit :

- Attendez quelques minutes, puis renvoyez votre demande. La capacité peut changer fréquemment.
- Envoyez une nouvelle demande avec un nombre réduit d'instances. Par exemple, si vous faites une demande simple pour lancer 15 instances, essayez de faire 3 demandes pour 5 instances ou 15 demandes pour 1 instance à la place.
- Si vous lancez une instance, soumettez une nouvelle demande sans spécifier de zone de disponibilité.
- Si vous lancez une instance, envoyez une nouvelle demande en utilisant un type d'instance différent (que vous pouvez redimensionner à un stade ultérieur). Pour de plus amples informations, veuillez consulter [Modifier le type d'instance](#).
- Si vous lancez des instances dans un groupe de placement du cluster, vous pouvez recevoir une erreur de capacité insuffisante. Pour de plus amples informations, veuillez consulter [Utilisation des groupes de placement](#).

La configuration demandée n'est actuellement pas prise en charge.
Consultez la documentation pour voir les configurations prises en charge.

Description

Vous obtenez l'erreur `Unsupported` lorsque vous essayez de lancer une nouvelle instance, car la configuration de l'instance n'est pas prise en charge.

Cause

Le message d'erreur fournit des informations supplémentaires. Par exemple, un type d'instance ou une option d'achat d'instance peut ne pas être prise en charge dans la région ou la zone de disponibilité spécifiée.

Solution

Essayez une autre configuration d'instance. Pour rechercher un type d'instance qui répond à vos besoins, consultez [Rechercher un type d'instance Amazon EC2](#).

Mise hors service immédiate de l'instance

Description

Votre instance passe de l'état `pending` à l'état `terminated`.

Cause

Voici quelques raisons qui expliquent pourquoi une instance peut se terminer immédiatement :

- Vous avez dépassé vos limites de volumes EBS. Pour de plus amples informations, veuillez consulter [Limites de volume d'instance](#).
- Un instantané EBS est corrompu.
- Le volume EBS racine est chiffré et vous n'êtes pas autorisé à accéder à la clé KMS pour le déchiffrement.
- Un instantané spécifié dans le mappage de périphérique de stockage en mode bloc pour l'AMI est chiffré et vous ne disposez pas des autorisations nécessaires pour accéder à la clé KMS pour la déchiffrer, ou vous n'avez pas accès à la clé KMS pour chiffrer les volumes restaurés.
- L'AMI basée sur le stockage d'instance que vous avez utilisée pour lancer l'instance ne possède par une partie obligatoire (un fichier `image.part.xx`).

Pour de plus amples informations, veuillez récupérer le motif de résiliation à l'aide de l'une des méthodes suivantes.

Pour obtenir la cause de la résiliation à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez instances, puis choisissez l'instance.
3. Dans le premier onglet, recherchez le motif en regard de State transition reason (Motif de transition de l'état).

Pour obtenir le motif du licenciement à l'aide du AWS Command Line Interface

1. Utilisez la commande [describe-instances](#) et spécifiez l'ID de l'instance.

```
aws ec2 describe-instances --instance-id instance_id
```

2. Vérifiez la réponse JSON renvoyée par la commande et notez les valeurs de l'élément de réponse StateReason.

Le bloc de code suivant présente un exemple d'élément de réponse StateReason.

```
"StateReason": {  
  "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",  
  "Code": "Server.InternalError"  
},
```

Pour obtenir le motif du licenciement en utilisant AWS CloudTrail

Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#) dans le Guide de AWS CloudTrail l'utilisateur.

Solution

En fonction de la cause de la résiliation, exécutez l'une des actions suivantes :

- **Client.VolumeLimitExceeded: Volume limit exceeded** — Supprimez les volumes inutilisés. Vous pouvez [envoyer une demande](#) d'augmentation de votre limite de volumes.
- **Client.InternalError: Client error on launch**— Assurez-vous que vous disposez des autorisations requises pour accéder aux volumes AWS KMS keys utilisés pour déchiffrer et

chiffrer. Pour de plus amples informations, veuillez consulter [Utilisation des politiques de clé AWS KMS](#) dans le AWS Key Management Service Guide du développeur.

Autorisations insuffisantes

Description

Vous obtenez l'erreur "*errorMessage*": "You are not authorized to perform this operation." lorsque vous essayez de lancer une nouvelle instance et que le lancement échoue.

Cause

Si cette erreur s'affiche lorsque vous essayez de lancer une instance, cela signifie que vous ne disposez pas des autorisations IAM requises pour lancer l'instance.

Les autorisations manquantes possibles incluent :

- `ec2:RunInstances`
- `iam:PassRole`

D'autres autorisations peuvent également être manquantes. Pour obtenir la liste des autorisations requises pour lancer une instance, consultez les exemples de politiques IAM sous [Exemple : utiliser l'assistant de lancement d'instances d'EC2](#) et [Instances de lancement \(RunInstances\)](#).

Solution

Pour résoudre le problème :

- Si vous faites des demandes en tant qu'utilisateur IAM, vérifiez que vous avez les autorisation suivantes :
 - `ec2:RunInstances` avec une ressource générique (« * »)
 - `iam:PassRole` avec la ressource correspondant à l'ARN du rôle (par exemple, `arn:aws:iam::999999999999:role/ExampleRoleName`)
- Si vous ne disposez pas des autorisations précédentes, [modifiez la politique IAM](#) associée au rôle ou à l'utilisateur IAM pour ajouter les autorisations requises manquantes.

Si votre problème persiste et que vous recevez toujours un message d'erreur d'échec de lancement, vous pouvez décoder le message d'échec d'autorisation inclus dans l'erreur. Le message

décodé inclut les autorisations qui ne figurent pas dans la politique IAM. Pour plus d'informations, consultez [Comment décodé un message d'échec d'autorisation après avoir reçu une erreur « UnauthorizedOperation » lors du lancement d'une instance EC2 ?](#)

Utilisation élevée du processeur peu après le démarrage de Windows (instances Windows uniquement)

Note

Ce conseil de résolution des problèmes concerne uniquement les instances Windows.

Si Windows Update est défini sur Rechercher des mises à jour mais me laisser choisir s'il convient de les télécharger et de les installer (paramètre de l'instance par défaut), cette vérification peut consommer entre 50 % et 99 % des ressources d'UC sur l'instance. Si cette consommation de l'UC est problématique pour vos applications, vous pouvez modifier manuellement les paramètres de Windows dans le Panneau de configuration ou vous pouvez utiliser le script suivant dans le champ des données utilisateur Amazon EC2 :

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 3 /f net stop wuauclt net start wuauclt
```

Lorsque vous exécutez ce script, spécifiez une valeur pour /d. La valeur par défaut est 3. Les valeurs possibles sont notamment les suivantes :

1. Ne jamais rechercher des mises à jour
2. Rechercher des mises à jour mais me laisser choisir s'il convient de les télécharger et de les installer
3. Télécharger des mises à jour mais me laisser choisir s'il convient de les installer
4. Installer les mises à jour automatiquement

Après avoir modifié les données utilisateur de votre instance, vous pouvez exécuter celle-ci. Pour plus d'informations, consultez [Exécuter des commandes sur votre instance Windows au lancement](#).

Résoudre les problèmes de connexion à votre instance Linux

Les informations suivantes et les erreurs courantes peuvent vous aider à résoudre les problèmes de connexion à votre instance Linux.

Problèmes de connexion

- [Causes courantes des problèmes de connexion](#)
- [Erreur de connexion à votre instance : connexion expirée](#)
- [Erreur : impossible de charger la clé... Attente : N'IMPORTE QUELLE CLÉ PRIVÉE](#)
- [Erreur : clé de l'utilisateur non reconnue par le serveur](#)
- [Erreur : autorisation refusée ou connexion fermée par \[instance\] port 22](#)
- [Erreur : fichier de clé privée non protégé](#)
- [Erreur : La clé privée doit commencer par « -----BEGIN RSA PRIVATE KEY----- » et se terminer par « -----END RSA PRIVATE KEY----- »](#)
- [Erreur : le serveur a refusé notre clé ou Aucune méthode d'authentification prise en charge disponible](#)
- [Impossible d'envoyer une commande ping à l'instance](#)
- [Erreur : le serveur a fermé la connexion réseau de manière inopinée](#)
- [Erreur : échec de la validation de la clé d'hôte pour EC2 Instance Connect](#)
- [Impossible de se connecter à une instance Ubuntu à l'aide de EC2 Instance Connect](#)
- [J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Linux ?](#)

Causes courantes des problèmes de connexion

Nous vous recommandons de commencer à résoudre les problèmes de connexion aux instances en vérifiant que vous avez correctement effectué les tâches suivantes.

Vérifiez le nom d'utilisateur de votre instance

Vous pouvez vous connecter à votre instance en utilisant le nom d'utilisateur de votre compte utilisateur ou le nom d'utilisateur par défaut de l'AMI que vous avez utilisée pour lancer votre instance.

- Obtenez le nom d'utilisateur de votre compte utilisateur.

Pour plus d'informations sur la création d'un compte utilisateur, consultez [Gérez les utilisateurs du système sur votre instance Linux](#).

- Obtenir le nom d'utilisateur par défaut pour l'AMI que vous avez utilisée pour lancer votre instance :

AMI utilisée pour lancer l'instance	Nom d'utilisateur par défaut
AL2023	ec2-user
Amazon Linux 2	
Amazon Linux	
CentOS	centos ou ec2-user
Debian	admin
Fedora	fedora ou ec2-user
RHEL	ec2-user ou root
SUSE	ec2-user ou root
Ubuntu	ubuntu
Oracle	ec2-user
Bitnami	bitnami
Rocky Linux	rocky
Autre	Vérifiez auprès du fournisseur de l'AMI

Vérifiez que les règles de votre groupe de sécurité autorisent le trafic

Vérifiez que le groupe de sécurité associé à votre instance autorise le trafic SSH entrant à partir de votre adresse IP. Le groupe de sécurité par défaut pour le VPC n'autorise pas le trafic SSH entrant par défaut. Le groupe de sécurité créé par l'assistant de lancement d'instance autorise le trafic SSH entrant par défaut. Pour savoir comment ajouter une règle pour le trafic SSH entrant vers votre instance Linux, consultez [Règles pour la connexion à des instances à partir de votre](#)

[ordinateur](#). Pour connaître les étapes à vérifier, consultez [Erreur de connexion à votre instance : connexion expirée](#).

Vérifiez que votre instance est prête

Une fois l'instance lancée, il peut falloir quelques minutes pour qu'elle soit prête pour que vous puissiez vous y connecter. Vérifiez votre instance pour vous assurer qu'elle est en cours d'exécution et qu'elle a réussi ses vérifications d'état.

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Vérifiez les paramètres suivants :
 - a. Dans la colonne État de l'instance, vérifiez que l'état de votre instance est `running`.
 - b. Dans la colonne Contrôle des statuts, vérifiez que votre instance a passé avec succès les deux vérifications de statut.

Vérifiez que vous avez répondu à toutes les conditions préalables pour vous connecter.

Assurez-vous de disposer de toutes les informations dont vous avez besoin pour vous connecter. Pour plus d'informations, consultez [Connectez-vous à votre instance Linux](#).

Pour connaître les prérequis spécifiques aux types de connexion, tels que SSH, EC2 Instance Connect, OpenSSH, PuTTY, etc., consultez les options suivantes.

Linux ou macOS X

Si le système d'exploitation de votre ordinateur local est Linux ou macOS X, vérifiez les prérequis spécifiques pour les options de connexion suivantes :

- [Client SSH](#)
- [EC2 Instance Connect](#)
- [AWS Systems Manager Gestionnaire de sessions](#)

Windows

Si le système d'exploitation de votre ordinateur local est Windows, vérifiez les prérequis spécifiques pour les options de connexion suivantes :

- [OpenSSH](#)

- [PuTTY](#)
- [AWS Systems Manager Gestionnaire de sessions](#)
- [WSL \(Windows Subsystem for Linux\)](#)

Erreur de connexion à votre instance : connexion expirée

Si vous essayez de vous connecter à votre instance et vous obtenez le message d'erreur `Network error: Connection timed out` ou `Error connecting to [instance], reason: -> Connection timed out: connect`, essayez ce qui suit :

Vérifiez les règles du groupe de sécurité.

Vous avez besoin d'un groupe de sécurité qui permet le trafic entrant à partir de votre adresse IPv4 publique de votre ordinateur local sur le même port.

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Sous l'onglet Sécurité au bas de la page de la console, sous Règles entrantes, vérifiez la liste des règles en vigueur pour l'instance sélectionnée.
 - Pour les instances Linux : vérifiez qu'il existe une règle qui permet le trafic de votre ordinateur local au port 22 (SSH).
 - Pour les instances Windows : vérifiez qu'il existe une règle qui permet le trafic de votre ordinateur local au port 3389 (RDP).

Si votre groupe de sécurité ne possède pas de règle qui permet le trafic entrant à partir de votre ordinateur local, ajoutez une règle à votre règle de sécurité. Pour plus d'informations, consultez [Règles pour la connexion à des instances à partir de votre ordinateur](#).

4. Pour connaître la règle qui autorise le trafic entrant, consultez la Source. Si la valeur est une adresse IP unique et si l'adresse IP n'est pas statique, une nouvelle adresse IP sera attribuée chaque fois que vous redémarrerez votre ordinateur. Cela aura pour conséquence que la règle n'inclut pas le trafic d'adresses IP de votre ordinateur. Il se peut que l'adresse IP ne soit pas statique si votre ordinateur est sur un réseau d'entreprise, si vous vous connectez via un fournisseur de services Internet (ISP), ou si l'adresse IP de votre ordinateur est dynamique et change chaque fois que vous redémarrez votre ordinateur. Pour vous assurer que votre règle de groupe de sécurité autorise le trafic entrant provenant de votre ordinateur local, au lieu de

spécifier une adresse IP unique pour Source, au lieu de spécifier la plage d'adresses IP utilisées par vos ordinateurs clients.

Pour plus d'informations sur les règles des groupes de sécurité, consultez la rubrique [Règles des groupes de sécurité](#) dans le Guide de l'utilisateur de Amazon VPC.

Vérifiez la table de routage pour le sous-réseau.

Vous avez besoin d'un itinéraire qui envoie tout le trafic destiné à l'extérieur du VPC vers la passerelle Internet du VPC.

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Sous l'onglet Mise en réseau, notez les valeurs de l'ID VPC et de l'ID de sous-réseau.
4. Ouvrez la console Amazon VPC sur <https://console.aws.amazon.com/vpc/>.
5. Dans le panneau de navigation, choisissez Passerelles Internet. Vérifiez qu'il existe une passerelle Internet attachée à votre VPC. Sinon, choisissez Créer une passerelle Internet, entrez un nom pour la passerelle Internet et choisissez Créer une passerelle Internet. Ensuite, pour la passerelle Internet que vous avez créée, choisissez Actions, Attacher au VPC, sélectionnez votre VPC, puis choisissez Attacher la passerelle Internet pour l'attacher à votre VPC.
6. Dans le panneau de navigation, sélectionnez Sous-réseaux, puis sélectionnez votre sous-réseau.
7. Dans l'onglet Table de routage, vérifiez qu'il existe une route avec $0.0.0.0/0$ comme destination et la passerelle Internet pour votre VPC comme cible. Si vous vous connectez à votre instance à l'aide de son adresse IPv6, vérifiez qu'il existe une route pour tout le trafic IPv6 ($::/0$) qui pointe vers la passerelle Internet. Sinon, procédez comme suit :
 - a. Choisissez l'ID de la table de routage (rtb-xxxxxxx) pour accéder à cette dernière.
 - b. Dans l'onglet Routes, choisissez Edit routes (Modifier les routes). Choisissez Add route (Ajouter une route) et utilisez $0.0.0.0/0$ comme destination et la passerelle Internet comme cible. Pour IPv6, choisissez Add route (Ajouter une route) et utilisez $::/0$ comme destination et la passerelle Internet comme cible.
 - c. Choisissez Save routes (Enregistrer les routes).

Vérifiez la liste de contrôle d'accès (ACL) du réseau pour le sous-réseau.

Les listes ACL de réseau doivent autoriser le trafic entrant à partir de votre adresse IP locale sur le port 22 (pour les instances Linux) ou le port 3389 (pour les instances Windows). Elles doivent également autoriser le trafic sortant vers les ports éphémères (1024-65535).

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Subnets.
3. Sélectionnez votre sous-réseau.
4. Dans la page ACL réseau, pour Règles entrantes, vérifiez que les règles autorisent le trafic entrant à partir de votre ordinateur sur le port requis. Sinon, supprimez ou modifiez la règle qui bloque le trafic.
5. Pour Règles sortantes, vérifiez que les règles autorisent le trafic vers votre ordinateur sur les ports éphémères. Sinon, supprimez ou modifiez la règle qui bloque le trafic.

Si votre ordinateur se trouve sur un réseau d'entreprise

Demandez à votre administrateur de réseau si le pare-feu interne permet le trafic entrant et sortant à partir de votre ordinateur sur le port 22 (pour les instances Linux) ou le port 3389 (pour les instances Windows).

Si vous avez un pare-feu sur votre ordinateur, vérifiez s'il permet le trafic entrant et sortant à partir de votre ordinateur sur le port 22 (pour les instances Linux) ou le port 3389 (pour les instances Windows).

Vérifiez que votre instance possède une adresse IPv4 publique.

Si non, vous pouvez associer une adresse IP Elastic à votre instance. Pour plus d'informations, consultez [Adresses IP Elastic](#).

Vérifiez la charge de l'UC sur votre instance. Il se peut que le serveur soit surchargé.

AWS fournit automatiquement des données telles que CloudWatch les métriques Amazon et le statut de l'instance, que vous pouvez utiliser pour connaître la charge du processeur de votre instance et, si nécessaire, ajuster la manière dont vos charges sont gérées. Pour plus d'informations, consultez [Surveillez vos instances à l'aide de CloudWatch](#).

- Si votre charge est variable, vous pouvez automatiquement effectuer des mises à l'échelle ascendantes et descendantes de vos instances en utilisant l'[Auto Scaling](#) et l'[Elastic Load Balancing](#).
- Si votre charge augmente régulièrement, vous pouvez passer à un type d'instance plus important. Pour plus d'informations, consultez [Modifier le type d'instance](#).

Pour vous connecter à votre instance à l'aide d'une adresse IPv6, vérifiez les points suivants :

- Votre sous-réseau doit être associé à une table de routage ayant une route pour le trafic IPv6 (: : /0) vers une passerelle Internet.
- Vos règles de groupe de sécurité doivent autoriser le trafic entrant à partir de votre adresse IPv6 locale sur le port approprié (22 pour Linux et 3389 pour Windows).
- Vos règles ACL réseau doivent autoriser le trafic IPv6 entrant et sortant.
- Si vous avez lancé votre instance à partir d'une AMI plus ancienne, elle n'est peut-être pas configurée pour DHCPv6 (les adresses IPv6 ne sont pas automatiquement reconnues sur l'interface réseau). Pour plus d'informations, consultez [Configuration d'IPv6 sur vos instances](#) dans le Guide de l'utilisateur Amazon VPC.
- Votre ordinateur local doit avoir une adresse IPv6 et doit être configuré pour utiliser IPv6.

Erreur : impossible de charger la clé... Attente : N'IMPORTE QUELLE CLÉ PRIVÉE

Si vous essayez de vous connecter à votre instance et obtenez le message d'erreur `unable to load key ... Expecting: ANY PRIVATE KEY`, le fichier dans lequel la clé privée est stockée est mal configuré. Si le fichier de clé privée se termine par `.pem`, il est peut-être toujours mal configuré. Une cause possible de configuration incorrecte d'un fichier de clé privée est l'absence d'un certificat.

Si le fichier de clé privée est mal configuré, suivez ces étapes pour corriger l'erreur.

1. Créez une nouvelle paire de clés. Pour plus d'informations, consultez [Créer une paire de clés à l'aide d'Amazon EC2](#).

Note

Sinon, vous pouvez créer une nouvelle key pair à l'aide d'un outil tiers. Pour plus d'informations, consultez [Créer une paire de clés à l'aide d'un outil tiers et importer la clé publique dans Amazon EC2](#).

2. Ajoutez la nouvelle paire de clés à votre instance. Pour plus d'informations, consultez [J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Linux ?](#).
3. Connectez-vous à votre instance à l'aide de la nouvelle paire de clés.

Erreur : clé de l'utilisateur non reconnue par le serveur

Si vous utilisez SSH pour vous connecter à votre instance

- Utilisez `ssh -vvv` pour obtenir des informations très détaillées sur le débogage en vous connectant :

```
ssh -vvv -i path/key-pair-name.pem instance-user-name@ec2-203-0-113-25.compute-1.amazonaws.com
```

L'exemple de données de sortie suivant montre que vous pouvez voir si vous étiez en train de vous connecter à votre instance avec une clé qui n'était pas reconnue par le serveur.

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
```

```
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Si vous utilisez PuTTY pour vous connecter à votre instance

- Vérifiez que votre fichier de clé privée (.pem) a été converti au format reconnu par PuTTY (.ppk). Pour plus d'informations sur la conversion de votre clé privée, consultez [Connexion à votre instance Linux à partir de Windows à l'aide de PuTTY](#).

 Note

Dans PuTTYgen, chargez votre fichier de clé privée et sélectionnez Enregistrer la clé privée plutôt que Générer.

- Vérifiez que vous vous connectez avec le nom utilisateur approprié pour votre AMI. Saisissez le nom d'utilisateur dans le champ Nom d'hôte de la fenêtre Configuration de PuTTY.

AMI utilisée pour lancer l'instance	Nom d'utilisateur par défaut
AL2023	ec2-user
Amazon Linux 2	
Amazon Linux	
CentOS	centos ou ec2-user
Debian	admin

AMI utilisée pour lancer l'instance	Nom d'utilisateur par défaut
Fedora	fedora ou ec2-user
RHEL	ec2-user ou root
SUSE	ec2-user ou root
Ubuntu	ubuntu
Oracle	ec2-user
Bitnami	bitnami
Rocky Linux	rocky
Autre	Vérifiez auprès du fournisseur de l'AMI

- Vérifiez que vous avez une règle entrante de groupe de sécurité pour permettre le trafic entrant vers le port approprié. Pour plus d'informations, consultez [Règles pour la connexion à des instances à partir de votre ordinateur](#).

Erreur : autorisation refusée ou connexion fermée par [instance] port 22

Si vous vous connectez à votre instance à l'aide de SSH et que vous obtenez l'une des erreurs suivantes, `Host key not found in [directory]`, `Permission denied (publickey)`, `Authentication failed`, `permission denied` ou `Connection closed by [instance] port 22`, vérifiez que vous vous connectez avec le nom d'utilisateur approprié pour votre AMI et que vous avez indiqué le bonne clé privée (fichier `.pem`) pour votre instance).

Les noms d'utilisateur appropriés sont comme suit :

AMI utilisée pour lancer l'instance	Nom d'utilisateur par défaut
AL2023	ec2-user
Amazon Linux 2	
Amazon Linux	

AMI utilisée pour lancer l'instance	Nom d'utilisateur par défaut
CentOS	centos ou ec2-user
Debian	admin
Fedora	fedora ou ec2-user
RHEL	ec2-user ou root
SUSE	ec2-user ou root
Ubuntu	ubuntu
Oracle	ec2-user
Bitnami	bitnami
Rocky Linux	rocky
Autre	Vérifiez auprès du fournisseur de l'AMI

Par exemple, pour utiliser un client SSH et vous connecter à une instance Amazon Linux, utilisez la commande suivante :

```
ssh -i /path/key-pair-name.pem instance-user-name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Confirmez que vous utilisez le fichier de clé privée qui correspond à la paire de clés que vous avez sélectionnée lorsque vous avez lancé l'instance.

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances, puis sélectionnez votre instance.
3. Sous l'onglet Détails, sous Détails de l'instance, vérifiez la valeur Nom de la paire de clés.
4. Si vous n'avez pas spécifié une paire de clés lorsque vous avez lancé l'instance, vous pouvez mettre fin à l'instance et lancer une nouvelle instance en vous assurant de spécifier une paire de clés. S'il s'agit d'une instance que vous avez utilisée, mais que vous n'avez plus le fichier .pem pour votre paire de clés, vous pouvez remplacer la paire de clés par une nouvelle. Pour

plus d'informations, consultez [J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Linux ?](#).

Si vous avez généré votre propre paire de clés, assurez-vous que votre générateur de clés est configuré pour créer des clés RSA. Les clés DSA ne sont pas acceptées.

Si vous obtenez une erreur `Permission denied` (`publickey`) et qu'aucune des réponses ci-dessus ne s'applique (par exemple, vous avez pu vous connecter précédemment), les autorisations sur le répertoire de base de votre instance a peut-être été modifiées. Les autorisations pour `/home/instance-user-name/.ssh/authorized_keys` doivent être limitées au propriétaire uniquement.

Pour vérifier les autorisations sur votre instance

1. Arrêtez votre instance et détachez le volume racine. Pour plus d'informations, consultez [Arrêtez et démarrez les instances Amazon EC2](#).
2. Lancez une instance temporaire dans la même zone de disponibilité que votre instance actuelle (utilisez une AMI similaire ou la même AMI que vous avez utilisée pour votre instance actuelle) et attachez le volume racine à l'instance temporaire.
3. Connectez-vous à l'instance temporaire, créez un point de montage et montez le volume que vous avez joint.
4. A partir de l'instance temporaire, vérifiez les autorisations du répertoire `/home/instance-user-name` du volume attaché. Si nécessaire, modifiez les autorisations comme suit :

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. Démontez le volume, détachez-le de l'instance temporaire et attachez-le de nouveau à l'instance originale. Assurez-vous que vous avez spécifié le bon nom de périphérique pour le volume racine, par exemple, `/dev/xvda`.
6. Démarrez votre instance. Si vous n'avez plus besoin de l'instance temporaire, vous pouvez la mettre en service.

Erreur : fichier de clé privée non protégé

Votre fichier de clé privée doit être protégé des opérations de lecture et d'écriture des autres utilisateurs. Si n'importe qui sauf vous peut lire ou écrire sur votre clé privée, alors SSH ignore votre clé et vous voyez le message d'avertissement suivant.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: UNPROTECTED PRIVATE KEY FILE!           @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Si vous voyez un message similaire lorsque vous essayez de vous connecter à votre instance, examinez la première ligne du message d'erreur pour vérifier que vous utilisez la bonne clé publique pour votre instance. L'exemple ci-dessus utilise la clé privée `.ssh/my_private_key.pem` avec les autorisations sur les fichiers de `0777` ce qui permet à n'importe qui de lire ou écrire sur ce fichier. Ce niveau d'autorisation n'est pas sûr du tout, donc SSH ignore cette clé.

Si vous vous connectez à partir de macOS ou Linux, exécutez la commande suivante pour corriger cette erreur en remplaçant le chemin par celui de votre fichier de clé privée.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Si vous vous connectez à partir de Windows, exécutez les étapes suivantes sur votre ordinateur local.

1. Accédez au fichier `.pem`.
2. Cliquez avec le bouton droit de la souris sur le fichier `.pem` et sélectionnez **Propriétés**.
3. Choisissez l'onglet **Security (Sécurité)**.
4. Sélectionnez **Avancé**.
5. Vérifiez que vous êtes le propriétaire du fichier. Si ce n'est pas le cas, changez le propriétaire avec votre nom d'utilisateur.
6. Sélectionnez **Désactiver l'héritage et Supprimer toutes les autorisations héritées de cet objet**.
7. Sélectionnez **Ajouter**, Sélectionnez un principal, saisissez votre nom d'utilisateur et sélectionnez **OK**.

8. À partir de la fenêtre Entrée d'autorisation, attribuez les autorisations Lire et sélectionnez OK.
9. Cliquez sur Apply (Appliquer) afin de garantir l'enregistrement de tous les paramètres.
10. Sélectionnez OK pour fermer la fenêtre Paramètres de sécurité avancés.
11. Sélectionnez OK pour fermer la fenêtre Propriétés.
12. Vous devriez être en mesure de vous connecter à votre instance Linux à partir de Windows via SSH.

À partir d'une invite de commande Windows, exécutez la commande suivante.

1. À partir de l'invite de commande, accédez à l'emplacement du chemin de fichier de votre fichier .pem.
2. Exécutez la commande suivante pour réinitialiser et supprimer les autorisations explicites :

```
icacls.exe $path /reset
```

3. Exécutez la commande suivante pour accorder à l'utilisateur actuel les autorisations de lecture :

```
icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
```

4. Exécutez la commande suivante pour désactiver l'héritage et supprimer les autorisations héritées.

```
icacls.exe $path /inheritance:r
```

5. Vous devriez être en mesure de vous connecter à votre instance Linux à partir de Windows via SSH.

Erreur : La clé privée doit commencer par « -----BEGIN RSA PRIVATE KEY----- » et se terminer par « -----END RSA PRIVATE KEY----- »

Si vous utilisez un outil tiers, tel que ssh-keygen, pour créer une paire de clés RSA, il génère la clé privée au format de clé OpenSSH. Lorsque vous vous connectez à votre instance, si vous utilisez la clé privée au format OpenSSH pour déchiffrer le mot de passe, vous obtenez l'erreur `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`.

Pour résoudre cette erreur, la clé privée doit être au format PEM. Utilisez la commande suivante pour créer la clé privée au format PEM :

```
ssh-keygen -m PEM
```

Erreur : le serveur a refusé notre clé ou Aucune méthode d'authentification prise en charge disponible

Si vous utilisez PuTTY pour vous connecter à votre instance et que vous obtenez l'une des erreurs suivantes, Erreur : Le serveur a refusé votre clé ou Erreur : Méthodes d'authentification disponibles non prises en charge, vérifiez que vous vous connectez avec le nom d'utilisateur approprié pour votre AMI. Entrez le nom d'utilisateur dans le champ Nom d'utilisateur de la fenêtre Configuration de PuTTY.

Les noms d'utilisateur appropriés sont comme suit :

AMI utilisée pour lancer l'instance	Nom d'utilisateur par défaut
AL2023	ec2-user
Amazon Linux 2	
Amazon Linux	
CentOS	centos ou ec2-user
Debian	admin
Fedora	fedora ou ec2-user
RHEL	ec2-user ou root
SUSE	ec2-user ou root
Ubuntu	ubuntu
Oracle	ec2-user
Bitnami	bitnami

AMI utilisée pour lancer l'instance	Nom d'utilisateur par défaut
Rocky Linux	rocky
Autre	Vérifiez auprès du fournisseur de l'AMI

Vous devez également vérifier que :

- Utilisez-vous la dernière version de PuTTY. Pour plus d'informations, consultez la [page Web PuTTY](#).
- Votre fichier de clé privée (.pem) a été bien converti au format reconnu par PuTTY (.ppk). Pour plus d'informations sur la conversion de votre clé privée, consultez [Connexion à votre instance Linux à partir de Windows à l'aide de PuTTY](#).

Impossible d'envoyer une commande ping à l'instance

La commande ping est un type de trafic ICMP. Si vous ne pouvez pas pinger votre instance, assurez-vous que vos règles entrantes de groupe de sécurité autorisent le trafic ICMP pour le message Echo Request de toutes les sources, ou de l'ordinateur ou de l'instance à partir desquels vous émettez la commande.

Si vous ne pouvez pas fournir une commande ping à partir de votre instance, assurez-vous que vos règles sortantes de groupe de sécurité autorisent le trafic ICMP pour le message Echo Request vers toutes les destinations ou vers l'hôte que vous essayez de pinger.

Les commandes Ping peuvent également être bloquées par un pare-feu ou un délai d'attente en raison de latence réseau ou de problèmes matériels. Vous devez consulter votre réseau local ou votre administrateur système pour obtenir de l'aide sur la résolution des problèmes supplémentaires.

Erreur : le serveur a fermé la connexion réseau de manière inopinée

Si vous vous connectez à votre instance via PuTTY et que vous recevez le message d'erreur « Le serveur a fermé la connexion réseau de manière inopinée », vérifiez que vous avez activé le paramètre keepalive dans la page de Connexion de la Configuration PuTTY, afin d'éviter de vous faire déconnecter. Certains serveurs déconnectent les clients lorsqu'ils n'ont pas reçu de données dans une période de temps spécifiée. Réglez les secondes entre keepalives à 59 secondes.

Si vous éprouvez encore des difficultés après avoir activé les keepalives, essayez de désactiver l'algorithme de Nagle dans la page de Connexion de la Configuration PuTTY.

Erreur : échec de la validation de la clé d'hôte pour EC2 Instance Connect

Si vous faites pivoter les clés d'hôte de votre instance, les nouvelles clés d'hôte ne sont pas automatiquement téléchargées dans la base de données de clés d'hôte AWS fiables. Cela provoque l'échec de la validation de clé d'hôte lorsque vous essayez de vous connecter à votre instance à l'aide du client EC2 Instance Connect basé sur le navigateur et vous ne parvenez pas à vous connecter à votre instance.

Pour résoudre cette erreur, vous devez exécuter le script `eic_harvest_hostkeys` sur votre instance, qui télécharge votre nouvelle clé d'hôte vers EC2 Instance Connect. Le script se trouve sur `/opt/aws/bin/` sur les instances Amazon Linux 2 et sur `/usr/share/ec2-instance-connect/` sur les instances Ubuntu.

Amazon Linux 2

Pour résoudre l'erreur de validation de clé d'hôte ayant échoué sur une instance Amazon Linux 2

1. Connectez-vous à votre instance à l'aide de SSH.

Vous pouvez vous connecter en utilisant la CLI EC2 Instance Connect ou la paire de clés SSH attribuée à votre instance lors de son lancement, ainsi que le nom d'utilisateur par défaut de l'AMI utilisée pour lancer votre instance. Pour Amazon Linux 2, le nom d'utilisateur par défaut est `ec2-user`.

Par exemple, si votre instance a été lancée avec Amazon Linux 2, que le nom DNS public de votre instance est `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` et que la paire de clés est `my_ec2_private_key.pem`, utilisez la commande suivante pour établir une connexion SSH à votre instance :

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez [Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#).

2. Accédez au dossier suivant.

```
[ec2-user ~]$ cd /opt/aws/bin/
```

3. Exécutez la commande suivante sur votre instance.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Notez qu'un appel réussi n'entraîne pas obligatoirement une sortie.

Vous pouvez désormais utiliser le client EC2 Instance Connect basé sur le navigateur pour vous connecter à votre instance.

Ubuntu

Pour résoudre l'erreur de validation de clé d'hôte ayant échoué sur une instance Ubuntu

1. Connectez-vous à votre instance à l'aide de SSH.

Vous pouvez vous connecter en utilisant la CLI EC2 Instance Connect ou la paire de clés SSH attribuée à votre instance lors de son lancement, ainsi que le nom d'utilisateur par défaut de l'AMI utilisée pour lancer votre instance. Pour Ubuntu, le nom d'utilisateur par défaut est `ubuntu`.

Par exemple, si votre instance a été lancée avec Ubuntu, que le nom DNS public de votre instance est `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` et que la paire de clés est `my_ec2_private_key.pem`, utilisez la commande suivante pour établir une connexion SSH à votre instance :

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Pour plus d'informations sur la connexion à votre instance, consultez [Connexion à votre instance Linux depuis Linux ou macOS à l'aide de SSH](#).

2. Accédez au dossier suivant.

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Exécutez la commande suivante sur votre instance.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Notez qu'un appel réussi n'entraîne pas obligatoirement une sortie.

Vous pouvez désormais utiliser le client EC2 Instance Connect basé sur le navigateur pour vous connecter à votre instance.

Impossible de se connecter à une instance Ubuntu à l'aide de EC2 Instance Connect

Si vous utilisez EC2 Instance Connect pour vous connecter à votre instance Ubuntu et que vous obtenez une erreur lorsque vous tentez de vous connecter, vous pouvez utiliser les informations suivantes pour tenter de résoudre le problème.

Cause possible

Le package `ec2-instance-connect` sur l'instance n'est pas la dernière version.

Solution

Mettre à jour le package `ec2-instance-connect` sur l'instance vers la dernière version, comme suit :

1. [Se connecter](#) à votre instance en utilisant une méthode autre que EC2 Instance Connect.
2. Exécuter la commande suivante sur votre instance pour mettre à jour le package `ec2-instance-connect` vers la dernière version.

```
apt update && apt upgrade
```

J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Linux ?

Si vous perdez la clé privée pour une instance basée sur des volumes EBS, vous pouvez à nouveau accéder à votre instance. Vous devez arrêter l'instance, détacher son volume racine et l'attacher à une autre instance en tant que volume de données, modifier le fichier `authorized_keys` avec une nouvelle clé publique, replacer le volume dans l'instance d'origine et redémarrer l'instance. Pour plus

d'informations sur le lancement et l'arrêt des instances, ainsi que sur la connexion aux instances, consultez [Cycle de vie d'une instance](#).

Cette procédure est prise en charge uniquement pour des instances avec des volumes racine EBS. Si l'appareil racine est un volume de stockage d'instance, vous ne pouvez pas utiliser cette procédure pour rétablir l'accès à votre instance ; vous devez disposer de la clé privée pour vous connecter à l'instance. Pour déterminer le type d'appareil racine de votre instance, ouvrez la console Amazon EC2, choisissez Instances, sélectionnez l'instance, choisissez l'onglet Stockage, et dans la section Détails de l'appareil racine, vérifiez la valeur du Type d'appareil racine.

La valeur est EBS ou INSTANCE-STORE.

En plus des étapes suivantes, il existe d'autres façons de vous connecter à votre instance Linux en cas de perte de votre clé privée. Pour de plus amples informations, veuillez consulter [Comment puis-je me connecter à mon instance Amazon EC2 si j'ai perdu ma paire de clés SSH après son lancement initial ?](#)

Étapes de connexion à une instance basée sur des volumes EBS avec une paire de clés différente

- [Étape 1 : Créer une nouvelle paire de clés](#)
- [Étape 2 : Obtenir des informations sur l'instance d'origine et son volume racine](#)
- [Étape 3 : Arrêter l'instance d'origine](#)
- [Étape 4 : Lancer une instance temporaire](#)
- [Étape 5 : Détacher le volume racine de l'instance d'origine et l'attacher à l'instance temporaire](#)
- [Étape 6 : Ajouter la nouvelle clé publique `authorized_keys` sur le volume d'origine monté sur l'instance temporaire](#)
- [Étape 7 : Démontez et détachez le volume d'origine de l'instance temporaire, puis le reconnectez à l'instance d'origine](#)
- [Étape 8 : Se connecter à l'instance d'origine à l'aide de la nouvelle paire de clés](#)
- [Étape 9 : nettoyer](#)

Étape 1 : Créer une nouvelle paire de clés

Créer une nouvelle paire de clés à l'aide de la console Amazon EC2 ou d'un outil tiers. Si vous souhaitez nommer votre nouvelle paire de clés exactement comme la clé privée perdue, vous devez commencer par supprimer la paire de clés existante. Pour de plus amples informations sur la création

d'une paire de clés, veuillez consulter [Créer une paire de clés à l'aide d'Amazon EC2](#) ou [Créer une paire de clés à l'aide d'un outil tiers et importer la clé publique dans Amazon EC2](#).

Étape 2 : Obtenir des informations sur l'instance d'origine et son volume racine

Notez les informations suivantes, car vous en aurez besoin pour effectuer cette procédure.

Pour obtenir des informations sur votre instance d'origine

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Choisissez Instances dans le panneau de navigation, puis sélectionnez l'instance à laquelle vous souhaitez vous connecter. (Cette instance est qualifiée d'instance d'origine.)
3. Sous l'onglet Details (Détails), notez l'ID d'instance et l'ID d'AMI.
4. Sous l'onglet Networking (Réseaux), notez la zone de disponibilité.
5. Sous l'onglet Storage (Stockage), sous Root device name (Nom du périphérique racine), notez le nom du périphérique pour le volume racine (par exemple, /dev/xvda). Ensuite, sous Block devices (Bloquer les périphériques), recherchez le nom du périphérique et notez l'ID de volume (par exemple, vol-0a1234b5678c910de).

Étape 3 : Arrêter l'instance d'origine

Choisissez État de l'instance, Arrêter l'instance. Si cette option est désactivée, l'instance est déjà arrêtée ou son périphérique racine est un volume de stockage d'instance.

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instance sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

Étape 4 : Lancer une instance temporaire

New console

Pour lancer une instance temporaire

1. Dans le volet de navigation, choisissez Instances, puis Launch instances (Lancer des instances).
2. Dans la section Name and tags (Noms et identifications), pour Name (Nom), saisissez Temporary (Temporaire).
3. Dans Application and OS Images (Images d'applications et de systèmes d'exploitation), sélectionnez la même AMI que celle utilisée pour lancer l'instance d'origine. Si l'AMI n'est pas disponible, vous pouvez créer une AMI à utiliser depuis l'instance arrêtée. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).
4. Dans la section Instance type (Type d'instance), sélectionnez le type d'instance par défaut.
5. Dans la section Key pair (Paire de clés), pour Key pair name (Nom de la paire de clés), sélectionnez une paire de clés existante ou créez-en une.
6. Dans la section Network settings (Paramètres réseau), choisissez Edit (Modifier), puis pour Subnet (Sous-réseau), sélectionnez un sous-réseau dans la même zone de disponibilité que celle de l'instance d'origine.
7. Dans le panneau Summary (Récapitulatif), choisissez Launch (Lancer).

Old console

Sélectionnez Launch instances (Lancer des instances), puis utilisez l'assistant de lancement pour lancer une instance temporaire avec les options suivantes :

- Dans la page Choisir une AMI, sélectionnez la même AMI que celle utilisée pour lancer l'instance d'origine. Si l'AMI n'est pas disponible, vous pouvez créer une AMI à utiliser depuis l'instance arrêtée. Pour plus d'informations, consultez [Création d'une AMI basée sur Amazon EBS](#).
- Sur la page Choisir un type d'instance, conservez le type d'instance par défaut sélectionné par l'assistant.
- Dans la page Configurer les détails de l'instance, spécifiez la même zone de disponibilité que l'instance d'origine. Si vous lancez une instance dans un VPC, sélectionnez un sous-réseau dans cette zone de disponibilité.

- Sur la page Ajouter des balises, ajoutez la balise Name=Temporary à l'instance pour indiquer qu'il s'agit d'une instance temporaire.
- Sur la page Review (Vérification), choisissez Launch (Lancer). Sélectionnez la paire de clés que vous avez créée à l'étape 1, puis sélectionnez Launch instances (Lancer les instances).

Étape 5 : Détacher le volume racine de l'instance d'origine et l'attacher à l'instance temporaire

1. Dans le panneau de navigation, sélectionnez Volumes, puis le volume du périphérique racine pour l'instance d'origine (vous avez noté l'ID de volume au cours d'une étape précédente). Choisissez Actions, Detach Volume (Détacher un volume), puis choisissez Detach (Détacher). Attendez que l'état du volume devienne `available`. (Vous devrez peut-être sélectionner l'icône Actualiser.)
2. Tandis que le volume est toujours sélectionné, choisissez Actions, puis choisissez Attach volume (Attacher un volume). Sélectionnez l'ID d'instance de l'instance temporaire, notez le nom du périphérique spécifié dans Device name (Nom du périphérique) (par exemple, `/dev/sdf`), puis sélectionnez Attach volume (Attacher un volume).

Note

Si vous avez lancé votre instance d'origine à partir d'une AWS Marketplace AMI et que votre volume contient des AWS Marketplace codes, vous devez d'abord arrêter l'instance temporaire avant de pouvoir attacher le volume.

Étape 6 : Ajouter la nouvelle clé publique **authorized_keys** sur le volume d'origine monté sur l'instance temporaire

1. Connectez-vous à l'instance temporaire.
2. À partir de l'instance temporaire, montez le volume que vous avez attaché à l'instance afin de pouvoir accéder au système de fichiers. Par exemple, si le nom du périphérique est `/dev/sdf`, utilisez les commandes suivantes pour monter le volume en tant que `/mnt/tempvol`.

Note

Le nom du périphérique peut apparaître différemment sur votre instance. Par exemple, les périphériques montés en tant que `/dev/sdf` peuvent également s'afficher en tant que `/dev/xvdf` sur l'instance. Certaines versions de Red Hat (ou ses variantes, comme CentOS) peuvent même incrémenter la lettre finale de quatre caractères, et `/dev/sdf` devient `/dev/xvdk`.

- a. Utilisez la commande `lsblk` pour déterminer si le volume est divisé.

```
[ec2-user ~]$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda        202:0    0   8G  0 disk
##xvda1    202:1    0   8G  0 part /
xvdf        202:80   0  101G  0 disk
##xvdf1    202:81   0  101G  0 part
xvdg        202:96   0   30G  0 disk
```

Dans l'exemple précédent, `/dev/xvda` et `/dev/xvdf` sont des volumes partitionnés, mais `/dev/xvdg` ne l'est pas. Si votre volume est partitionné, vous montez la partition (`/dev/xvdf1`) au lieu du périphérique brut (`/dev/xvdf`) au cours des étapes suivantes.

- b. Créez un répertoire temporaire pour monter le volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

- c. Montez le volume (ou la partition) sur le point de montage temporaire, en utilisant le nom du volume ou du périphérique que vous avez identifié plus tôt. La commande requise dépend du système de fichiers de votre système d'exploitation. Notez que le nom du périphérique peut apparaître différemment sur votre instance. Reportez-vous à l'étape 6 de [note](#) pour plus d'informations.

- Amazon Linux, Ubuntu et Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 et RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

Note

Si vous obtenez une erreur indiquant que le système de fichiers est endommagé, exécutez la commande suivante pour utiliser l'utilitaire fsck afin de rechercher les erreurs dans votre système de fichiers et de les résoudre.

```
[ec2-user ~]$ sudo fsck /dev/xvdf1
```

3. À partir de l'instance temporaire, utilisez la commande suivante pour mettre à jour `authorized_keys` sur le volume monté avec la nouvelle clé publique de `authorized_keys` pour l'instance temporaire.

Important

Les exemples suivants utilisent le nom d'utilisateur Amazon Linux `ec2-user`. Vous devrez peut-être modifier le nom d'utilisateur, par exemple, `ubuntu` pour les instances Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Une fois que cette étape est correctement effectuée, vous pouvez passer à l'étape suivante.

(Facultatif) Sinon, si vous n'êtes pas autorisé à modifier des fichiers dans `/mnt/tempvol`, vous devez mettre à jour le fichier à l'aide de la commande `sudo`, puis vérifier les autorisations sur le fichier afin de vous assurer que vous êtes en mesure de vous connecter à l'instance d'origine. Pour vérifier les autorisations sur le fichier, utilisez la commande suivante.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw----- 1 222 500 398 Sep 13 22:54 authorized_keys
```

Dans cet exemple, **222** est l'ID d'utilisateur et **500** est l'ID de groupe. Utilisez ensuite la commande `sudo` pour ré-exécuter la commande `copy` ayant échoué.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Exécutez à nouveau la commande suivante pour déterminer si les autorisations ont été modifiées.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Si l'ID d'utilisateur et l'ID de groupe ont été modifiés, utilisez la commande suivante pour les restaurer.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Étape 7 : Démontez et détachez le volume d'origine de l'instance temporaire, puis le reconnecter à l'instance d'origine

1. À partir de l'instance temporaire, démontez le volume que vous avez attaché afin de pouvoir l'attacher à nouveau à l'instance d'origine. Par exemple, utilisez la commande suivante pour démonter le volume situé dans `/mnt/tempvol`.

```
[ec2-user ~]$ sudo umount /mnt/tempvol
```

2. Détachez le volume de l'instance temporaire (vous l'avez démonté à l'étape précédente) : dans la console Amazon EC2, choisissez Volumes dans le panneau de navigation, sélectionnez le volume du périphérique racine de l'instance d'origine (vous avez noté l'ID de volume à l'étape précédente), sélectionnez Actions, Detach volume (Détacher un volume), puis Detach (Détacher). Attendez que l'état du volume devienne `available`. (Vous devrez peut-être sélectionner l'icône Actualiser.)
3. Rattachez le volume à l'instance d'origine : le volume étant toujours sélectionné, choisissez Actions, Attach volume (Attacher un volume). Sélectionnez l'ID d'instance de l'instance d'origine, précisez le nom de l'appareil que vous avez noté précédemment au cours de l'[étape 2](#) pour l'attachement de l'appareil racine d'origine (`/dev/sda1` ou `/dev/xvda`), puis choisissez Attach volume (Attacher un volume).

⚠ Important

Si vous ne spécifiez pas le même nom de périphérique que pour l'attachement original, vous ne pourrez pas démarrer l'instance d'origine. Amazon EC2 s'attend à ce que le volume du périphérique racine soit sda1 ou /dev/xvda.

Étape 8 : Se connecter à l'instance d'origine à l'aide de la nouvelle paire de clés

Sélectionnez l'instance d'origine, choisissez État de l'instance, Démarrer l'instance. Lorsque l'état de l'instance est `running`, vous pouvez vous y connecter à l'aide du fichier de clé privée de votre nouvelle paire de clés.

i Note

Si le nom de votre paire de clés et du fichier de clé privée correspondant est différent du nom de la paire de clés initiale, veillez à spécifier le nom du nouveau fichier de clé privée lorsque vous vous connectez à votre instance.

Étape 9 : nettoyer

(Facultatif) Vous pouvez mettre fin à l'instance temporaire si vous n'en avez plus besoin.

Sélectionnez l'instance temporaire, puis Instance State (État de l'instance) et `Terminate instance` (Résilier l'instance).

Résoudre les problèmes de connexion à votre instance Windows

Les informations suivantes et les erreurs courantes peuvent vous aider à résoudre les problèmes de connexion à votre instance Windows.

Problèmes de connexion

- [Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant](#)
- [Erreur lors de l'utilisation du client RDP macOS](#)
- [RDP affiche un écran noir au lieu du bureau](#)
- [Impossible de se connecter à distance à une instance avec un utilisateur autre qu'un administrateur](#)

- [Résolution des problèmes de bureau à distance à l'aide de AWS Systems Manager](#)
- [Activation du Bureau à distance sur une instance EC2 avec le Registre à distance](#)
- [J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Windows ?](#)

Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant

Essayez d'exécuter l'opération suivante pour résoudre les problèmes liés à votre connexion à votre instance :

- Vérifiez que vous utilisez le nom d'hôte DNS public adéquat. (Dans la console Amazon EC2, sélectionnez l'instance et vérifiez DNS public (IPv4) dans le volet des détails.) Si votre instance est un VPC et que le nom DNS public ne s'affiche pas, vous devez activer les noms d'hôtes DNS. Pour plus d'informations, consultez [DNS attributes for your VPC](#) (Attributs DNS pour votre VPC) dans le Guide de l'utilisateur d'Amazon VPC.
- Vérifiez que votre instance dispose d'une adresse IPv4 publique. Si non, vous pouvez associer une adresse IP Elastic à votre instance. Pour de plus amples informations, veuillez consulter [Adresses IP Elastic](#).
- Pour vous connecter à votre instance à l'aide d'une adresse IPv6, vérifiez que votre ordinateur local dispose d'une adresse IPv6 et qu'il est configuré pour utiliser IPv6. Pour plus d'informations, consultez [Configuration d'IPv6 sur vos instances](#) dans le Guide de l'utilisateur Amazon VPC.
- Vérifiez que votre groupe de sécurité contient une règle qui autorise l'accès RDP.
- Si vous avez copié le mot de passe, mais que vous obtenez l'erreur `Your credentials did not work`, essayez de le saisir manuellement lorsque vous y êtes invité. Il est possible que vous ayez oublié un caractère ou ajouté une espace supplémentaire lorsque vous avez copié le mot de passe.
- Vérifiez que l'instance a réussi les contrôles d'état. Pour plus d'informations, consultez [Contrôles de statut pour vos instances](#) et [the section called "Échec des vérifications d'état sous Linux"](#).
- Vérifiez que la table de routage du sous-réseau contient une route qui envoie tout le trafic destiné à l'extérieur du VPC vers la passerelle Internet du VPC. Pour plus d'informations, consultez [Créer une table de routage personnalisée](#) (Passerelles Internet) dans le Amazon VPC Guide de l'utilisateur.
- Vérifiez que le pare-feu Windows, ou tout autre logiciel de pare-feu, ne bloque pas le trafic RDP vers l'instance. Nous vous recommandons de désactiver le pare-feu Windows et le contrôle d'accès à votre instance à l'aide des règles des groupes de sécurité. Vous pouvez [AWSSupport-TroubleshootRDP](#) utiliser pour [disable the Windows Firewall profiles using SSM Agent](#). Pour

désactiver le pare-feu Windows sur une instance Windows qui n'est pas configurée pour AWS Systems Manager [AWSSupport-ExecuteEC2Rescue](#), utilisez ou suivez les étapes manuelles suivantes :

Étapes manuelles

1. Arrêtez l'instance affectée et détachez son volume racine.
2. Lancez une instance temporaire dans la même zone de disponibilité que l'instance affectée.

Warning

Si votre instance temporaire est basée sur la même AMI que l'instance d'origine, vous devez effectuer des étapes supplémentaires. Dans le cas contraire, vous ne serez pas en mesure de démarrer l'instance d'origine après la restauration de son volume racine en raison d'une collision de signature de disque. Sinon, sélectionnez une autre AMI pour l'instance temporaire. Par exemple, si l'instance d'origine utilise l'AMI AWS Windows pour Windows Server 2016, lancez l'instance temporaire à l'aide de l'AMI AWS Windows pour Windows Server 2019.

3. Attachez le volume racine de l'instance affectée à cette instance temporaire. Connectez-vous à l'instance temporaire, ouvrez l'utilitaire Gestion des disques et mettez le lecteur en ligne.
4. Ouvrez Regedit et sélectionnez HKEY_LOCAL_MACHINE. Dans le menu File (Fichier), choisissez Load Hive (Charger Hive). Sélectionnez le lecteur, ouvrez le fichier `Windows\System32\config\SYSTEM` et spécifiez un nom de clé lorsque vous y êtes invité (vous pouvez utiliser n'importe quel nom).
5. Sélectionnez la clé que vous venez de charger et naviguez jusqu'à `ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy`. Pour chaque clé portant un nom au format `xxxxProfile`, sélectionnez la clé et passez `EnableFirewall` de 1 à 0. Sélectionnez à nouveau la clé, puis dans le menu File (Fichier), sélectionnez Unload Hive (Décharger Hive).
6. (Facultatif) Si votre instance temporaire est basée sur la même AMI que l'instance d'origine, vous devez effectuer les étapes suivantes. Dans le cas contraire, vous ne serez pas en mesure de démarrer l'instance d'origine après la restauration de son volume racine en raison d'une collision de signature de disque.

⚠ Warning

La procédure suivante décrit comment modifier le Registre Windows à l'aide de l'Éditeur de Registre. Si vous n'êtes pas familier avec le Registre Windows ou comment apporter des modifications en toute sécurité à l'aide de l'Éditeur de Registre, consultez [Configurer le registre](#).

- a. Ouvrez une invite de commande, saisissez regedit.exe, puis appuyez sur Entrée.
- b. Dans Editeur de registre, choisissez HKEY_LOCAL_MACHINE dans le menu contextuel (clic droit), puis choisissez Rechercher.
- c. Cliquez sur Windows Boot Manager, puis choisissez Rechercher suivant.
- d. Choisissez la clé nommée 11000001. Cette clé est apparentée à la clé que vous avez trouvée à l'étape précédente.
- e. Dans le volet droit, choisissez Element, puis Modifier à partir du menu contextuel (clic droit).
- f. Localisez la signature du disque de quatre octets au décalage 0x38 dans les données. Inversez les octets pour créer la signature du disque et l'écrire. Par exemple, la signature de disque représentée par les données suivantes est E9EB3AA5 :

```
...  
0030  00 00 00 00 01 00 00 00  
0038  A5 3A EB E9 00 00 00 00  
0040  00 00 00 00 00 00 00 00  
...
```

- g. Dans une fenêtre d'invite de commandes, exécutez la commande suivante pour démarrer Microsoft DiskPart.

```
diskpart
```

- h. Exécutez la DiskPart commande suivante pour sélectionner le volume. (Vous pouvez vérifier que le numéro de disque est 1 à l'aide de l'utilitaire Gestion des disques.

```
DISKPART> select disk 1
```

```
Disk 1 is now the selected disk.
```

- i. Exécutez la DiskPart commande suivante pour obtenir la signature du disque.

```
DISKPART> uniqueid disk
```

```
Disk ID: 0C764FA8
```

- j. Si la signature de disque affichée à l'étape précédente ne correspond pas à la signature de disque de BCD que vous avez notée plus tôt, utilisez la DiskPart commande suivante pour modifier la signature de disque afin qu'elle corresponde :

```
DISKPART> uniqueid disk id=E9EB3AA5
```

7. À l'aide de l'utilitaire Gestion des disques, déconnectez le lecteur.

Note

Le lecteur est automatiquement hors ligne si l'instance temporaire exécute le même système d'exploitation que l'instance concernée. Vous n'aurez donc pas besoin de le mettre hors ligne manuellement.

8. Détachez le volume de l'instance temporaire. Vous pouvez mettre l'instance temporaire hors service si vous n'en avez plus besoin.
9. Restaurez le volume racine de l'instance affectée en attachant celui-ci en tant que /dev/sda1.
10. Démarrez l'instance.

- Vérifiez que l'authentification au niveau du réseau est désactivée sur les instances qui ne font pas partie d'un domaine Active Directory (utilisez [AWSSupport-TroubleshootRDP](#) pour [disable NLA](#)).
- Vérifiez que le type de démarrage du service Remote Desktop (TermService) est automatique et que le service est démarré (utilisez [AWSSupport-TroubleshootRDP](#) pour [enable and start the RDP service](#)).
- Vérifiez que vous vous connectez au port RDP (Remote Desktop Protocol) approprié, qui est par défaut le port 3389 (utilisez [AWSSupport-TroubleshootRDP](#) pour [read the current RDP port](#) et [change it back to 3389](#)).
- Vérifiez que les connexions via le service Bureau à distance sont autorisées sur votre instance (utilisez [AWSSupport-TroubleshootRDP](#) pour [enable Remote Desktop connections](#)).

- Vérifiez que le mot de passe n'a pas expiré. Si c'est le cas, vous pouvez le réinitialiser. Pour plus d'informations, consultez [Réinitialisation d'un mot de passe administrateur Windows perdu ou expiré](#).
- Si vous tentez de vous connecter à l'aide d'un utilisateur que vous avez créé sur l'instance et que vous recevez le message d'erreur `The user cannot connect to the server due to insufficient access privileges`, vérifiez que vous avez autorisé l'utilisateur à se connecter localement. Pour plus d'informations, consultez [Accorder à un membre le droit de se connecter localement](#).
- Si vous tentez d'ouvrir un nombre de sessions RDP simultanées supérieur à la limite autorisée, votre session est mise hors service et le message suivant est renvoyé : `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost`. Par défaut, deux sessions RDP simultanées sont autorisées sur votre instance.

Erreur lors de l'utilisation du client RDP macOS

Si vous vous connectez à une instance Windows Server à l'aide du client Remote Desktop Connection sur le site Web de Microsoft, le message d'erreur suivant peut s'afficher :

```
Remote Desktop Connection cannot verify the identity of the computer that you want to connect to.
```

Téléchargez l'application Microsoft Remote Desktop à partir du Mac App Store et utilisez cette application pour vous connecter à votre instance.

RDP affiche un écran noir au lieu du bureau

Essayez ce qui suit pour résoudre ce problème :

- Consultez la sortie de la console pour plus d'informations. Pour obtenir la sortie de la console de votre instance à l'aide de la console Amazon EC2, sélectionnez l'instance, puis Actions, Surveiller et dépanner et Obtenir le journal système.
- Vérifiez que vous exécutez la version la plus récente de votre client RDP.
- Essayez les paramètres par défaut pour le client RDP. Pour plus d'informations, consultez [Remote Session Environment](#).
- Si vous utilisez la connexion au Bureau à distance, essayez de la démarrer avec l'option `/admin` comme suit.

```
mstsc /v:instance /admin
```

- Si le serveur exécute une application plein écran, il se peut qu'elle ait cessé de répondre. Utilisez Ctrl+Shift+Esc pour démarrer le Gestionnaire des tâches de Windows, puis fermez l'application.
- Si le serveur est sur-utilisé, il peut avoir cessé de répondre. Pour surveiller l'instance à l'aide de la console Amazon EC2, sélectionnez l'instance, puis sélectionnez l'onglet Surveillance. Si vous avez besoin d'attribuer une taille supérieure au type d'instance, consultez [Modifier le type d'instance](#).

Impossible de se connecter à distance à une instance avec un utilisateur autre qu'un administrateur

Si vous ne pouvez pas vous connecter à distance à une instance Windows avec un utilisateur qui n'est pas un compte administrateur, vérifiez que l'utilisateur est autorisé à se connecter localement. Consultez [Accorder à un utilisateur ou à un groupe le droit de se connecter localement aux contrôleurs de domaine du domaine](#).

Résolution des problèmes de bureau à distance à l'aide de AWS Systems Manager

Vous pouvez l'utiliser AWS Systems Manager pour résoudre les problèmes de connexion à votre instance Windows à l'aide du protocole RDP.

AWSSupport- Résoudre les problèmes liés au RDP

Le document d'automatisation AWSSupport -TroubleShootRDP permet à l'utilisateur de vérifier ou de modifier les paramètres courants de l'instance cible susceptibles d'avoir un impact sur les connexions RDP (Remote Desktop Protocol), tels que le port RDP, l'authentification de couche réseau (NLA) et les profils de pare-feu Windows. Par défaut, le document lit et produit les valeurs de ces paramètres.

Le document d'automatisation AWSSupport -TroubleShootRDP peut être utilisé avec les instances EC2, les instances sur site et les machines virtuelles (VM) activées pour être utilisées avec (instances gérées). AWS Systems Manager En outre, il peut également être utilisé avec des instances EC2 pour Windows Server qui ne sont pas activées pour une utilisation avec Systems Manager. Pour plus d'informations sur l'activation des instances à utiliser avec AWS Systems Manager, consultez la section [Nœuds gérés](#) dans le guide de AWS Systems Manager l'utilisateur.

Pour résoudre les problèmes à l'aide du document AWSSupport -TroubleshootRDP

1. Connectez-vous à la [console Systems Manager](#).
2. Vérifiez que vous êtes dans la même région que l'instance dégradée.
3. Dans le volet de navigation de gauche, choisissez Documents.
4. Sur l'onglet Owned by Amazon (Propriété d'Amazon), saisissez AWSSupport - TroubleshootRDP dans le champ de recherche. Lorsque le document AWSSupport - TroubleshootRDP apparaît, sélectionnez-le.
5. Sélectionnez Execute automation (Exécuter l'automatisation).
6. Pour Mode d'exécution, choisissez Exécution simple.
7. Pour les paramètres d'entrée InstanceId, activez Afficher le sélecteur d'instance interactif.
8. Sélectionnez votre instance Amazon EC2.
9. Consultez les [exemples](#), puis choisissez Exécuter.
10. Pour surveiller la progression de l'exécution, dans Statut de l'exécution, attendez que le statut passe de En attente à Réussite. Développez Sorties pour afficher les résultats. Pour afficher la sortie de chaque étape, dans Étapes exécutées, choisissez l'ID d'étape.

AWSSupport- Exemples de résolution des problèmes liés au RDP

Les exemples suivants vous montrent comment effectuer des tâches de dépannage courantes à l'aide de AWSSupport -TroubleShootRDP. Vous pouvez utiliser l'exemple de AWS CLI [start-automation-execution](#) commande ou le lien fourni vers le AWS Management Console.

Exemple Exemple : Vérifier le statut RDP actuel

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --parameters "InstanceId=instance_id, Action=Custom" --region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-TroubleshootRDP?region=region#documentVersion=$LATEST
```

Exemple Exemple : Désactiver le pare-feu Windows

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
  --parameters "InstanceId=instance_id, Action=Custom, Firewall=Disable" --
  region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
  TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Exemple Exemple : Désactiver l'authentification au niveau du réseau

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
  --parameters "InstanceId=instance_id, Action=Custom, NLASettingAction=Disable" --
  region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
  TroubleshootRDP?region=region_code#documentVersion
```

Exemple Exemple : Définir le type de démarrage du service RDP sur Automatique et démarrer le service RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
  --parameters "InstanceId=instance_id, Action=Custom, RDPServiceStartupType=Auto,
  RDPServiceAction=Start" --region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/
  AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
  $LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Exemple Exemple : Restaurer le port RDP par défaut (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
  --parameters "InstanceId=instance_id, Action=Custom, RDPPortAction=Modify" --
region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Exemple Exemple : Autoriser les connexions à distance

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
  --parameters "InstanceId=instance_id, Action=Custom, RemoteConnections=Enable" --
region region_code
```

AWS Systems Manager console :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport- Exécutez EC2 Rescue

Le document d'automatisation AWSSupport -ExecuteEC2Rescue utilise EC2Rescue pour Windows Server pour résoudre et restaurer automatiquement la connectivité des instances EC2 et les problèmes RDP. Pour plus d'informations, consultez [Exécuter l'outil EC2Rescue sur des instances inaccessibles](#).

Le document d'automatisation AWSSupport -ExecuteEC2Rescue nécessite l'arrêt et le redémarrage de l'instance. Systems Manager Automation arrête l'instance et crée une Amazon Machine Image (AMI). Les données stockées sur les volumes de stockage d'instance sont perdues. L'adresse IP publique est modifiée si vous n'utilisez pas une adresse IP Elastic. Pour plus d'informations, consultez [Exécuter l'outil EC2Rescue sur des instances inaccessibles](#) dans le Guide de l'utilisateur AWS Systems Manager .

Pour résoudre les problèmes liés à l'utilisation du document `AWSSupport-ExecuteEC2Rescue`

1. Ouvrez la [console Systems Manager](#).
2. Vérifiez que vous êtes dans la même région que l'instance Amazon EC2 dégradée.
3. Dans le panneau de navigation, choisissez Documents.
4. Recherchez et sélectionnez le document `AWSSupport-ExecuteEC2Rescue`, puis choisissez Exécuter l'automatisation.
5. Dans Execution mode (Mode d'exécution), choisissez Simple Execution (Exécution simple).
6. Dans la section Paramètres d'entrée, pour `UnreachableInstanceid`, entrez l'ID d'instance Amazon EC2 de l'instance inaccessible.
7. (Facultatif) Pour `LogDestination`, entrez le nom du bucket Amazon Simple Storage Service (Amazon S3) si vous souhaitez collecter les journaux du système d'exploitation pour le dépannage de votre instance Amazon EC2. Les journaux sont chargés automatiquement dans le compartiment spécifié.
8. Sélectionnez Execute (Exécuter).
9. Pour surveiller la progression de l'exécution, dans Execution statut (Statut de l'exécution), attendez que le statut passe de Pending (En attente) à Success (Succès). Développez Sorties pour afficher les résultats. Pour afficher la sortie de chaque étape, dans Executed Steps (Étapes exécutées), choisissez l'ID d'étape.

Activation du Bureau à distance sur une instance EC2 avec le Registre à distance

Si votre instance inaccessible n'est pas gérée par le gestionnaire de session de AWS Systems Manager, vous pouvez utiliser le registre distant pour activer Remote Desktop.

1. À partir de la console EC2, arrêtez l'instance inaccessible.
2. Détachez le volume racine de l'instance inaccessible et attachez-le à une instance accessible dans la même zone de disponibilité que le volume de stockage. Si vous n'avez pas d'instance accessible dans la même zone de disponibilité, lancez-en une. Notez le nom du périphérique du volume racine de l'instance inaccessible.
3. Sur l'instance accessible, ouvrez la Gestion des disques. Vous pouvez le faire en exécutant la commande suivante dans une fenêtre d'invite de commande.

```
diskmgmt.msc
```

4. Cliquez avec le bouton droit sur le volume récemment attaché provenant de l'instance inaccessible, puis sélectionnez En ligne.
5. Ouvrez l'Éditeur du Registre Windows. Vous pouvez le faire en exécutant la commande suivante dans une fenêtre d'invite de commande.

```
regedit
```

6. Dans l'Éditeur du Registre, choisissez HKEY_LOCAL_MACHINE, puis sélectionnez Fichier, Charger Hive.
7. Sélectionnez le lecteur du volume attaché, accédez à \Windows\System32\config\, sélectionnez SYSTEM, puis choisissez Ouvrir.
8. Dans Nom de clé, entrez un nom unique pour le répertoire de stockage et choisissez OK.
9. Sauvegardez la ruche du registre avant d'apporter des modifications au registre.
 - a. Dans l'arborescence de la console de l'Éditeur du Registre, sélectionnez le répertoire de stockage que vous avez chargé : HKEY_LOCAL_MACHINE*nom-de-votre-clé*.
 - b. Choisissez Fichier, Exporter.
 - c. Dans la boîte de dialogue Exporter un fichier du Registre, choisissez l'emplacement vers lequel vous souhaitez enregistrer la copie de sauvegarde, puis tapez un nom pour le fichier de sauvegarde dans le champ Nom du fichier.
 - d. Choisissez Enregistrer.
10. Dans l'Éditeur du Registre, accédez à HKEY_LOCAL_MACHINE*your key name*\ControlSet001\Control\Terminal Server, puis, dans le volet de détails, double-cliquez sur fDenyTSConnections.
11. Dans la zone Modifier la valeur DWORD, entrez 0 dans le champ Données de valeur.
12. Choisissez OK.

Note

Si la valeur du champ Données de valeur est 1, l'instance refusera les connexions au bureau à distance. La valeur 0 autorise les connexions au bureau à distance.

13. Dans l'Éditeur du Registre, choisissez HKEY_LOCAL_MACHINE*nom-de-votre-clé*, puis sélectionnez Fichier, Charger Hive.
14. Fermez l'Éditeur du Registre et la Gestion des disques.
15. À partir de la console EC2, détachez le volume de l'instance accessible et attachez-le à nouveau à l'instance inaccessible. Lorsque vous attachez le volume à l'instance inaccessible, saisissez le nom du périphérique que vous avez enregistré précédemment dans le champ Périphérique.
16. Redémarrez l'instance inaccessible.

J'ai perdu ma clé privée. Comment puis-je me connecter à mon instance Windows ?

Lorsque vous vous connectez à une instance Windows lancée récemment, vous déchiffrez le mot de passe du compte administrateur à l'aide de la clé privée de la paire de clés que vous avez spécifiée lors du lancement de l'instance.

Si vous perdez le mot de passe administrateur et que vous n'avez plus de clé privée, vous devez réinitialiser le mot de passe ou créer une nouvelle instance. Pour plus d'informations, consultez [Réinitialisation d'un mot de passe administrateur Windows perdu ou expiré](#). Pour connaître les étapes de réinitialisation du mot de passe à l'aide d'un document Systems Manager, consultez [Réinitialiser des mots de passe et des clés SSH sur des instances EC2](#) dans le Guide de l'utilisateur AWS Systems Manager .

Réinitialisation d'un mot de passe administrateur Windows perdu ou expiré

Note

Cette section s'applique uniquement aux instances Windows.

Si vous ne pouvez plus accéder à votre instance Amazon EC2 Windows, car le mot de passe administrateur Windows est perdu ou a expiré, vous pouvez réinitialiser le mot de passe.

Note

Il existe un document AWS Systems Manager d'automatisation qui applique automatiquement les étapes manuelles nécessaires pour réinitialiser le mot de passe de l'administrateur local. Pour plus d'informations, consultez la section [Réinitialiser les mots de passe et les clés SSH sur les instances EC2](#) dans le guide de l'AWS Systems Manager utilisateur.

Les méthodes manuelles pour réinitialiser le mot de passe administrateur utilisent EC2Launch v2, EC2Config ou EC2Launch.

- Pour toutes les AMI Windows prises en charge qui incluent l'agent EC2Launch v2, utilisez EC2Launch v2.
- Pour les AMI Windows antérieures à Windows Server 2016, utilisez le service EC2Config.
- Pour les AMI Windows Server 2016 et versions ultérieures, utilisez le service EC2Launch.

Ces procédures expliquent aussi comment vous connecter à une instance, si vous avez perdu la paire de clés qui a été utilisée pour créer l'instance. Amazon EC2 utilise une clé publique pour chiffrer une portion de données, telle qu'un mot de passe, et une clé privée pour déchiffrer les données. La clé publique et la clé privée constituent une paire de clés. Avec les instances Windows, vous utilisez une paire de clés pour obtenir le mot de passe administrateur, puis vous vous connectez à l'aide du protocole RDP.

Note

Si vous avez désactivé le compte d'administrateur local sur l'instance et que votre instance est configurée pour Systems Manager, vous pouvez également réactiver et réinitialiser votre mot de passe d'administrateur local à l'aide d'EC2Rescue et Run Command. Pour plus d'informations, voir [Utiliser EC2Rescue pour Windows Server avec la commande Run de Systems Manager](#).

Table des matières

- [Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Launch v2](#)
- [Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Config](#)

- [Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Launch](#)

Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Launch v2

Si vous avez perdu votre mot de passe administrateur Windows et que vous utilisez une AMI Windows prise en charge qui inclut l'agent EC2Launch v2, vous pouvez utiliser EC2Launch v2 pour générer un nouveau mot de passe.

Si vous utilisez une AMI Windows Server 2016 ou version ultérieure qui n'inclut pas l'agent EC2Launch v2, veuillez consulter [Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Launch](#).

Si vous utilisez une AMI Windows Server antérieure à Windows Server 2016 qui n'inclut pas l'agent EC2Launch v2, veuillez consulter [Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Config](#).

Note

Si vous avez désactivé le compte d'administrateur local sur l'instance et que votre instance est configurée pour Systems Manager, vous pouvez également réactiver et réinitialiser votre mot de passe d'administrateur local à l'aide d'EC2Rescue et Run Command. Pour plus d'informations, voir [Utiliser EC2Rescue pour Windows Server avec la commande Run de Systems Manager](#).

Note

Il existe un document AWS Systems Manager d'automatisation qui applique automatiquement les étapes manuelles nécessaires pour réinitialiser le mot de passe de l'administrateur local. Pour plus d'informations, consultez la section [Réinitialiser les mots de passe et les clés SSH sur les instances EC2](#) dans le guide de l'AWS Systems Manager utilisateur.

Pour réinitialiser votre mot de passe administrateur Windows avec EC2Launch v2, vous devez effectuer les opérations suivantes :

- [Étape 1 : vérifier que l'agent EC2Launch v2 est en cours d'exécution](#)
- [Étape 2 : Détacher le volume racine de l'instance](#)
- [Étape 3 : Attacher le volume à une instance temporaire](#)
- [Étape 4 : Supprimer le fichier .run-once.](#)
- [Étape 5 : Redémarrer l'instance originale](#)

Étape 1 : vérifier que l'agent EC2Launch v2 est en cours d'exécution

Avant d'essayer de réinitialiser le mot de passe administrateur, vérifiez que l'agent EC2Launch v2 est installé et en cours d'exécution. Vous utiliserez l'agent EC2Launch v2 pour réinitialiser le mot de passe administrateur ultérieurement dans cette section.

Pour vérifier que l'agent EC2Launch v2 est en cours d'exécution

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances, puis sélectionnez l'instance dont le mot de passe doit être réinitialisé. Cette instance s'appelle l'instance originale dans cette procédure.
3. Sélectionnez Actions, Surveiller et dépanner, Obtenir le journal système.
4. Recherchez l'entrée Launch EC2, par exemple Launch: EC2Launch v2 service v2.0.124. Si cette entrée s'affiche, cela signifie que le service EC2Launch v2 est en cours d'exécution.

Si le résultat du journal système est vide ou si l'agent EC2Launch v2 n'est pas en cours d'exécution, dépannez l'instance à l'aide du service de capture d'écran de la console d'instance. Pour plus d'informations, consultez [Création d'une capture d'écran d'une instance inaccessible](#).

Étape 2 : Détacher le volume racine de l'instance

Vous ne pouvez pas utiliser EC2Launch v2 pour réinitialiser un mot de passe administrateur si le volume sur lequel le mot de passe est stocké est attaché à une instance en tant que volume racine. Vous devez détacher le volume de l'instance originale avant de pouvoir l'attacher à une instance temporaire en tant que volume secondaire.

Détacher le volume racine de l'instance

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.

3. Sélectionnez l'instance qui nécessite une réinitialisation du mot de passe et choisissez État de l'instance, Arrêter l'instance. Une fois que le statut de l'instance est passé à Arrêtée, passez à l'étape suivante.
4. (Facultatif) Si vous disposez de la clé privée que vous avez spécifiée lors du lancement de cette instance, passez à l'étape suivante. Sinon, procédez comme suit pour remplacer l'instance par une nouvelle instance que vous lancez par une nouvelle paire de clés.
 - a. Créez une nouvelle paire de clés à l'aide de la console Amazon EC2. Si vous souhaitez nommer votre nouvelle paire de clés exactement comme la clé privée perdue, vous devez commencer par supprimer la paire de clés existante.
 - b. Sélectionnez l'instance à remplacer. Notez le type d'instance, le VPC, le sous-réseau, le groupe de sécurité et le rôle IAM de l'instance.
 - c. Choisissez Actions, Image and templates (Image et modèles), Create image (Créer une image). Saisissez le nom et la description de l'image, puis choisissez Créer l'image. Dans le panneau de navigation, sélectionnez AMI. Une fois le statut de l'image passé à disponible, passez à l'étape suivante.
 - d. Sélectionnez l'image et choisissez Actions, puis Lancement.
 - e. Terminez l'Assistant en sélectionnant le même type d'instance, VPC, sous-réseau, groupe de sécurité et le même rôle IAM que l'instance à remplacer, puis choisissez Lancement.
 - f. Lorsque vous y êtes invité, sélectionnez la paire de clés que vous avez créée pour la nouvelle instance, cochez la case de confirmation, puis sélectionnez Lancer des instances.
 - g. (Facultatif) Si l'instance d'origine a une adresse IP Elastic associée, associez-la à la nouvelle instance. Si l'instance d'origine comporte des volumes EBS en plus du volume racine, transférez-les vers la nouvelle instance.
5. Détachez le volume racine de l'instance d'origine comme suit :
 - a. Sélectionnez l'instance d'origine et cliquez sur l'onglet Stockage. Notez le nom du périphérique racine sous Nom du périphérique racine. Recherchez le volume portant ce nom de périphérique sous Bloquer les appareils, puis notez l'ID du volume.
 - b. Dans le panneau de navigation, choisissez Volumes.
 - c. Dans la liste des volumes, sélectionnez le volume que vous avez noté comme périphérique racine, puis choisissez Actions, Détacher le volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.
6. Si vous avez créé une nouvelle instance pour remplacer votre instance d'origine, vous pouvez mettre fin à l'instance d'origine dès maintenant. Ce n'est plus nécessaire. Pour le reste de cette

procédure, toutes les références à l'instance d'origine s'appliquent à la nouvelle instance que vous avez créée.

Étape 3 : Attacher le volume à une instance temporaire

Ensuite, lancez une instance temporaire et attachez-lui le volume en tant que volume secondaire. Il s'agit de l'instance que vous utilisez pour modifier le fichier de configuration.

Pour lancer une instance temporaire et attacher le volume

1. Lancez l'instance temporaire comme suit :
 - a. Dans le panneau de navigation, choisissez Instances, puis choisissez Lancer une instance, puis sélectionnez une AMI.

 Important

Pour éviter les collisions de signature de disque, vous devez sélectionner une AMI pour une autre version de Windows. Par exemple, si l'instance d'origine exécute Windows Server 2019, lancez l'instance temporaire à l'aide de l'AMI d'origine pour Windows Server 2016.

- b. Quittez le type d'instance par défaut, puis choisissez Suivant : configurer les détails de l'instance.
 - c. Dans la page Configurer les détails d'instance, pour Sous-réseau, sélectionnez la même zone de disponibilité que l'instance d'origine et choisissez Revoir et lancer.

 Important

Lancez une instance temporaire dans la même zone de disponibilité que l'instance d'origine. Si votre instance temporaire se trouve dans une zone de disponibilité différente, vous ne pouvez pas y attacher le volume racine de l'instance d'origine.

- d. Sur la page Review Instance Launch, sélectionnez Launch.
 - e. Lorsque vous y êtes invité, créez une nouvelle paire de clés, téléchargez-la dans un emplacement sûr de votre ordinateur, puis choisissez Lancer des instances.
2. Attachez le volume à l'instance temporaire en tant que volume secondaire, comme suit :

- a. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume que vous avez détaché de l'instance d'origine, et sélectionnez Actions, Attacher un volume.
- b. Dans la boîte de dialogue Attacher un volume, pour Instances, commencez par saisir le nom ou l'ID de votre instance temporaire, puis sélectionnez-la dans la liste.
- c. Pour Appareil, saisissez **xvdf** (s'il n'est pas déjà présent), puis choisissez Attacher.

Étape 4 : Supprimer le fichier .run-once.

Vous devez à présent supprimer le fichier `.run-once` du volume hors ligne attaché à l'instance. Cela permet à EC2Launch v2 d'exécuter toutes les tâches avec une fréquence de once, ce qui inclut la définition du mot de passe administrateur. Le chemin du fichier dans le volume secondaire que vous avez joint est similaire à `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

Pour supprimer le fichier `.run-once`

1. Ouvrez l'utilitaire de gestion des disques et mettez le lecteur en ligne en suivant ces instructions : [Rendre un volume Amazon EBS disponible pour utilisation](#).
2. Localisez le fichier `.run-once` sur le disque que vous avez mis en ligne.
3. Supprimez le fichier `.run-once`.

Important

Tous les scripts définis comme devant être exécutés une fois seront déclenchés par cette action.

Étape 5 : Redémarrer l'instance originale

Après avoir supprimé le fichier `.run-once`, rattachez le volume à l'instance originale en tant que volume racine et connectez-vous à l'instance en utilisant sa paire de clés pour récupérer le mot de passe administrateur.

1. Rattachez le volume à l'instance originale comme suit :
 - a. Dans le panneau de navigation, choisissez Volumes, sélectionnez le volume que vous avez détaché de l'instance temporaire, et sélectionnez Actions, Attacher un volume.

- b. Dans la boîte de dialogue Attacher un volume, pour Instances, saisissez le nom ou l'ID de votre instance d'origine, puis sélectionnez l'instance.
 - c. Pour Appareil, saisissez **/dev/sda1**.
 - d. Choisissez Attacher. Une fois le statut du volume passé à `in-use`, passez à l'étape suivante.
2. Dans le panneau de navigation, choisissez Instances. Sélectionnez l'instance d'origine et choisissez État de l'instance, Démarrer l'instance. Après que l'état de l'instance est passé à `Running`, passez à l'étape suivante.
 3. Récupérez votre nouveau mot de passe administrateur Windows à l'aide de la clé privée de la nouvelle paire de clés et connectez-vous à l'instance. Pour de plus amples informations, veuillez consulter [Connexion à votre instance Windows](#).

 Important

L'instance reçoit une nouvelle adresse IP publique après que vous l'arrêtez et la redémarrez. Veillez à vous connecter à l'instance à l'aide de son nom DNS public. Pour de plus amples informations, veuillez consulter [Cycle de vie d'une instance](#).

4. (Facultatif) Vous pouvez résilier l'instance temporaire si vous n'en avez plus besoin. Sélectionnez l'instance temporaire, puis choisissez État de l'instance et Résilier l'instance.

Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Config

Si vous avez oublié votre mot de passe administrateur Windows et que vous utilisez une AMI Windows antérieure à Windows Server 2016, vous pouvez utiliser l'agent EC2Config pour générer un nouveau mot de passe.

Si vous utilisez une AMI Windows Server 2016 ou ultérieure, veuillez consulter [Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Launch](#) ou, vous pouvez utiliser l'[outil EC2Rescue](#), qui utilise le service EC2Launch pour générer un nouveau mot de passe.

 Note

Si vous avez désactivé le compte d'administrateur local sur l'instance et que votre instance est configurée pour Systems Manager, vous pouvez également réactiver et réinitialiser votre

mot de passe d'administrateur local à l'aide d'EC2Rescue et Run Command. Pour plus d'informations, voir [Utiliser EC2Rescue pour Windows Server avec la commande Run de Systems Manager](#).

 Note

Il existe un document AWS Systems Manager d'automatisation qui applique automatiquement les étapes manuelles nécessaires pour réinitialiser le mot de passe de l'administrateur local. Pour plus d'informations, consultez la section [Réinitialiser les mots de passe et les clés SSH sur les instances EC2](#) dans le guide de l'AWS Systems Manager utilisateur.

Pour réinitialiser votre mot de passe administrateur Windows avec EC2Config, vous devez effectuer les opérations suivantes :

- [Étape 1 : Vérifier que le service EC2Config est en cours d'exécution.](#)
- [Étape 2 : Détacher le volume racine de l'instance](#)
- [Étape 3 : Attacher le volume à une instance temporaire](#)
- [Étape 4 : Modifier le fichier de configuration](#)
- [Étape 5 : Redémarrer l'instance originale](#)

Étape 1 : Vérifier que le service EC2Config est en cours d'exécution.

Avant d'essayer de réinitialiser le mot de passe administrateur, vérifiez que le service EC2Config est installé et en cours d'exécution. Vous utiliserez le service EC2Config pour réinitialiser le mot de passe administrateur ultérieurement dans cette section.

Pour vérifier que le service EC2Config est en cours d'exécution

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances, puis sélectionnez l'instance dont le mot de passe doit être réinitialisé. Cette instance s'appelle l'instance originale dans cette procédure.
3. Sélectionnez Actions, Monitor and troubleshoot (Surveiller et dépanner), Get system log (Obtenir le journal système).

(Ancienne console) Choisissez Actions, System Settings (Paramètres du système), Get system log (Obtenir le journal système).

4. Recherchez l'entrée Agent EC2, par exemple, EC2 Agent: Ec2Config service v3.18.1118. Si vous voyez cette entrée, le service EC2Config est en cours d'exécution.

Si le résultat du journal système est vide ou si le service EC2Config n'est pas en cours d'exécution, dépannez l'instance à l'aide du service de capture d'écran de la console d'instance. Pour plus d'informations, consultez [Création d'une capture d'écran d'une instance inaccessible](#).

Étape 2 : Détacher le volume racine de l'instance

Vous ne pouvez pas utiliser EC2Config pour réinitialiser un mot de passe administrateur si le volume sur lequel le mot de passe est stocké est attaché à une instance en tant que volume racine. Vous devez détacher le volume de l'instance originale avant de pouvoir l'attacher à une instance temporaire en tant que volume secondaire.

Détacher le volume racine de l'instance

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance qui nécessite une réinitialisation du mot de passe et choisissez État de l'instance, Arrêter l'instance. Une fois que le statut de l'instance est passé à Arrêtée, passez à l'étape suivante.
4. (Facultatif) Si vous disposez de la clé privée que vous avez spécifiée lors du lancement de cette instance, passez à l'étape suivante. Sinon, procédez comme suit pour remplacer l'instance par une nouvelle instance que vous lancez par une nouvelle paire de clés.
 - a. Créez une nouvelle paire de clés à l'aide de la console Amazon EC2. Si vous souhaitez nommer votre nouvelle paire de clés exactement comme la clé privée perdue, vous devez commencer par supprimer la paire de clés existante.
 - b. Sélectionnez l'instance à remplacer. Notez le type d'instance, le VPC, le sous-réseau, le groupe de sécurité et le rôle IAM de l'instance.
 - c. Choisissez Actions, Image and templates (Image et modèles), Create image (Créer une image). Saisissez le nom et la description de l'image, puis choisissez Créer l'image. Dans le panneau de navigation, sélectionnez AMI. Une fois le statut de l'image passé à disponible, passez à l'étape suivante.

- d. Sélectionnez l'image et choisissez Actions, puis Lancement.
 - e. Terminez l'Assistant en sélectionnant le même type d'instance, VPC, sous-réseau, groupe de sécurité et le même rôle IAM que l'instance à remplacer, puis choisissez Lancement.
 - f. Lorsque vous y êtes invité, sélectionnez la paire de clés que vous avez créée pour la nouvelle instance, cochez la case de confirmation, puis sélectionnez Lancer des instances.
 - g. (Facultatif) Si l'instance d'origine a une adresse IP Elastic associée, associez-la à la nouvelle instance. Si l'instance d'origine comporte des volumes EBS en plus du volume racine, transférez-les vers la nouvelle instance.
5. Détachez le volume racine de l'instance d'origine comme suit :
- a. Sélectionnez l'instance d'origine et cliquez sur l'onglet Stockage. Notez le nom du périphérique racine sous Nom du périphérique racine. Recherchez le volume portant ce nom de périphérique sous Bloquer les appareils, puis notez l'ID du volume.
 - b. Dans le panneau de navigation, choisissez Volumes.
 - c. Dans la liste des volumes, sélectionnez le volume que vous avez noté comme périphérique racine, puis choisissez Actions, Détacher le volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.
6. Si vous avez créé une nouvelle instance pour remplacer votre instance d'origine, vous pouvez mettre fin à l'instance d'origine dès maintenant. Ce n'est plus nécessaire. Pour le reste de cette procédure, toutes les références à l'instance d'origine s'appliquent à la nouvelle instance que vous avez créée.

Étape 3 : Attacher le volume à une instance temporaire

Ensuite, lancez une instance temporaire et attachez-lui le volume en tant que volume secondaire. Il s'agit de l'instance que vous utilisez pour modifier le fichier de configuration.

Pour lancer une instance temporaire et attacher le volume

1. Lancez l'instance temporaire comme suit :
 - a. Dans le panneau de navigation, choisissez Instances, puis choisissez Lancer une instance, puis sélectionnez une AMI.

⚠ Important

Pour éviter les collisions de signature de disque, vous devez sélectionner une AMI pour une autre version de Windows. Par exemple, si l'instance d'origine exécute Windows Server 2019, lancez l'instance temporaire à l'aide de l'AMI d'origine pour Windows Server 2016.

- b. Quittez le type d'instance par défaut, puis choisissez Suivant : configurer les détails de l'instance.
- c. Dans la page Configurer les détails d'instance, pour Sous-réseau, sélectionnez la même zone de disponibilité que l'instance d'origine et choisissez Revoir et lancer.

⚠ Important

Lancez une instance temporaire dans la même zone de disponibilité que l'instance d'origine. Si votre instance temporaire se trouve dans une zone de disponibilité différente, vous ne pouvez pas y attacher le volume racine de l'instance d'origine.

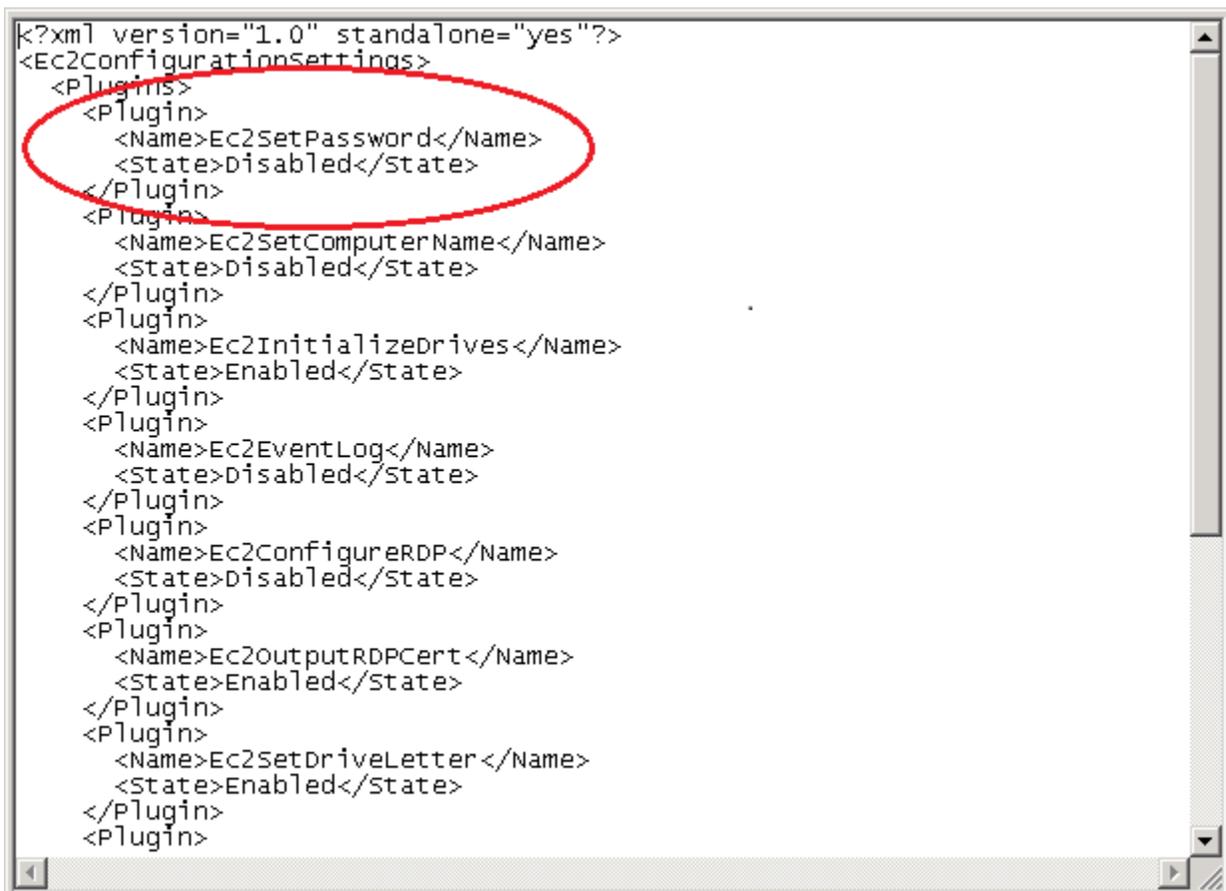
- d. Sur la page Review Instance Launch, sélectionnez Launch.
 - e. Lorsque vous y êtes invité, créez une nouvelle paire de clés, téléchargez-la dans un emplacement sûr de votre ordinateur, puis choisissez Lancer des instances.
2. Attachez le volume à l'instance temporaire en tant que volume secondaire, comme suit :
 - a. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume que vous avez détaché de l'instance d'origine, et sélectionnez Actions, Attacher un volume.
 - b. Dans la boîte de dialogue Attacher un volume, pour Instances, commencez par saisir le nom ou l'ID de votre instance temporaire, puis sélectionnez-la dans la liste.
 - c. Pour Appareil, saisissez **xvdf** (s'il n'est pas déjà présent), puis choisissez Attacher.

Étape 4 : Modifier le fichier de configuration

Après avoir attaché le volume à une instance temporaire en tant que volume secondaire, modifiez le plug-in Ec2SetPassword dans le fichier de configuration.

Pour modifier le fichier de configuration

1. Dans l'instance temporaire, modifiez le fichier de configuration sur le volume secondaire comme suit :
 - a. Lancez et connectez-vous à l'instance temporaire.
 - b. Suivez les instructions suivantes pour mettre le lecteur en ligne : [Rendre un volume Amazon EBS disponible pour utilisation](#).
 - c. Accédez au volume secondaire et ouvrez \Program Files\Amazon\Ec2ConfigService\Settings\config.xml à l'aide d'un éditeur de texte comme le Bloc-notes.
 - d. En haut du fichier, recherchez le plug-in portant le nom Ec2SetPassword, comme illustré dans la capture d'écran. Remplacez la valeur Disabled de l'état par Enabled et enregistrez le fichier.



```
<?xml version="1.0" standalone="yes"?>
<Ec2ConfigurationSettings>
  <Plugins>
    <Plugin>
      <Name>Ec2SetPassword</Name>
      <State>Disabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2SetComputerName</Name>
      <State>Disabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2InitializeDrives</Name>
      <State>Enabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2EventLog</Name>
      <State>Disabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2ConfigureRDP</Name>
      <State>Disabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2OutputRDPcert</Name>
      <State>Enabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2SetDriveLetter</Name>
      <State>Enabled</State>
    </Plugin>
    <Plugin>
  
```

2. Après avoir modifié le fichier de configuration, détachez le volume secondaire de l'instance temporaire comme suit :

- a. À l'aide de l'utilitaire Gestion des disques, déconnectez le volume.
- b. Déconnectez-vous de l'instance temporaire et revenez à la console Amazon EC2.
- c. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume, puis sélectionnez Actions, Détacher un volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.

Étape 5 : Redémarrer l'instance originale

Après avoir modifié le fichier de configuration, rattachiez le volume à l'instance originale en tant que volume racine et connectez-vous à l'instance en utilisant sa paire de clés pour récupérer le mot de passe administrateur.

1. Rattachez le volume à l'instance originale comme suit :
 - a. Dans le panneau de navigation, choisissez Volumes, sélectionnez le volume que vous avez détaché de l'instance temporaire, et sélectionnez Actions, Attacher un volume.
 - b. Dans la boîte de dialogue Attacher un volume, pour Instances, saisissez le nom ou l'ID de votre instance d'origine, puis sélectionnez l'instance.
 - c. Pour Appareil, saisissez **/dev/sda1**.
 - d. Choisissez Attacher. Une fois le statut du volume passé à in-use, passez à l'étape suivante.
2. Dans le panneau de navigation, choisissez Instances. Sélectionnez l'instance d'origine et choisissez État de l'instance, Démarrer l'instance. Après que l'état de l'instance est passé à Running, passez à l'étape suivante.
3. Récupérez votre nouveau mot de passe administrateur Windows à l'aide de la clé privée de la nouvelle paire de clés et connectez-vous à l'instance. Pour de plus amples informations, veuillez consulter [Connexion à votre instance Windows](#).

Important

L'instance reçoit une nouvelle adresse IP publique après que vous l'arrêtez et la redémarriez. Veillez à vous connecter à l'instance à l'aide de son nom DNS public. Pour de plus amples informations, veuillez consulter [Cycle de vie d'une instance](#).

4. (Facultatif) Vous pouvez résilier l'instance temporaire si vous n'en avez plus besoin. Sélectionnez l'instance temporaire, puis choisissez État de l'instance et Résilier l'instance.

Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Launch

Si vous avez oublié votre mot de passe administrateur Windows et que vous utilisez une AMI Windows Server 2016 ou ultérieure, vous pouvez utiliser l'[outil EC2Rescue](#) qui fait appel au service EC2Launch pour générer un nouveau mot de passe.

Si vous utilisez une AMI Windows Server 2016 ou ultérieure qui n'inclut pas l'agent EC2Launch v2, vous pouvez utiliser EC2Launch v2 pour générer un nouveau mot de passe.

Si vous utilisez une AMI Windows Server antérieure à Windows Server 2016, consultez [Réinitialisation d'un mot de passe administrateur Windows à l'aide d'EC2Config](#).

Warning

Lorsque vous arrêtez une instance, les données contenues sur les volumes de stockage d'instance sont effacées. Pour conserver les données provenant des volumes de stockage d'instances, sauvegardez-les sur un stockage permanent.

Note

Si vous avez désactivé le compte d'administrateur local sur l'instance et que votre instance est configurée pour Systems Manager, vous pouvez également réactiver et réinitialiser votre mot de passe d'administrateur local à l'aide d'EC2Rescue et Run Command. Pour plus d'informations, voir [Utiliser EC2Rescue pour Windows Server avec la commande Run de Systems Manager](#).

Note

Il existe un document AWS Systems Manager d'automatisation qui applique automatiquement les étapes manuelles nécessaires pour réinitialiser le mot de passe de l'administrateur local. Pour plus d'informations, consultez la section [Réinitialiser les mots](#)

[de passe et les clés SSH sur les instances EC2](#) dans le guide de l'AWS Systems Manager utilisateur.

Pour réinitialiser votre mot de passe administrateur Windows avec EC2Launch, vous devez effectuer les opérations suivantes :

- [Étape 1 : Détacher le volume racine de l'instance](#)
- [Étape 2 : Attacher le volume à une instance temporaire](#)
- [Étape 3 : Réinitialiser le mot de passe administrateur](#)
- [Étape 4 : Redémarrer l'instance originale](#)

Étape 1 : Détacher le volume racine de l'instance

Vous ne pouvez pas utiliser EC2Launch pour réinitialiser un mot de passe administrateur si le volume sur lequel le mot de passe est stocké est attaché à une instance en tant que volume racine. Vous devez détacher le volume de l'instance originale avant de pouvoir l'attacher à une instance temporaire en tant que volume secondaire.

Détacher le volume racine de l'instance

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance qui nécessite une réinitialisation du mot de passe et choisissez État de l'instance, Arrêter l'instance. Une fois que le statut de l'instance est passé à Arrêtée, passez à l'étape suivante.
4. (Facultatif) Si vous disposez de la clé privée que vous avez spécifiée lors du lancement de cette instance, passez à l'étape suivante. Sinon, procédez comme suit pour remplacer l'instance par une nouvelle instance que vous lancez par une nouvelle paire de clés.
 - a. Créez une nouvelle paire de clés à l'aide de la console Amazon EC2. Si vous souhaitez nommer votre nouvelle paire de clés exactement comme la clé privée perdue, vous devez commencer par supprimer la paire de clés existante.
 - b. Sélectionnez l'instance à remplacer. Notez le type d'instance, le VPC, le sous-réseau, le groupe de sécurité et le rôle IAM de l'instance.

- c. Choisissez Actions, Image and templates (Image et modèles), Create image (Créer une image). Saisissez le nom et la description de l'image, puis choisissez Créer l'image. Dans le panneau de navigation, sélectionnez AMI. Une fois le statut de l'image passé à disponible, passez à l'étape suivante.
 - d. Sélectionnez l'image et choisissez Actions, puis Lancement.
 - e. Terminez l'Assistant en sélectionnant le même type d'instance, VPC, sous-réseau, groupe de sécurité et le même rôle IAM que l'instance à remplacer, puis choisissez Lancement.
 - f. Lorsque vous y êtes invité, sélectionnez la paire de clés que vous avez créée pour la nouvelle instance, cochez la case de confirmation, puis sélectionnez Lancer des instances.
 - g. (Facultatif) Si l'instance d'origine a une adresse IP Elastic associée, associez-la à la nouvelle instance. Si l'instance d'origine comporte des volumes EBS en plus du volume racine, transférez-les vers la nouvelle instance.
5. Détachez le volume racine de l'instance d'origine comme suit :
- a. Sélectionnez l'instance d'origine et cliquez sur l'onglet Stockage. Notez le nom du périphérique racine sous Nom du périphérique racine. Recherchez le volume portant ce nom de périphérique sous Bloquer les appareils, puis notez l'ID du volume.
 - b. Dans le panneau de navigation, choisissez Volumes.
 - c. Dans la liste des volumes, sélectionnez le volume que vous avez noté comme périphérique racine, puis choisissez Actions, Détacher le volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.
6. Si vous avez créé une nouvelle instance pour remplacer votre instance d'origine, vous pouvez mettre fin à l'instance d'origine dès maintenant. Ce n'est plus nécessaire. Pour le reste de cette procédure, toutes les références à l'instance d'origine s'appliquent à la nouvelle instance que vous avez créée.

Étape 2 : Attacher le volume à une instance temporaire

Ensuite, lancez une instance temporaire et attachez-lui le volume en tant que volume secondaire. Il s'agit de l'instance que vous utilisez pour exécuter EC2Launch.

Pour lancer une instance temporaire et attacher le volume

1. Lancez l'instance temporaire comme suit :

- a. Dans le panneau de navigation, choisissez Instances, puis choisissez Lancer une instance, puis sélectionnez une AMI.

 Important

Pour éviter les collisions de signature de disque, vous devez sélectionner une AMI pour une autre version de Windows. Par exemple, si l'instance d'origine exécute Windows Server 2019, lancez l'instance temporaire à l'aide de l'AMI d'origine pour Windows Server 2016.

- b. Quittez le type d'instance par défaut, puis choisissez Suivant : configurer les détails de l'instance.
- c. Dans la page Configurer les détails d'instance, pour Sous-réseau, sélectionnez la même zone de disponibilité que l'instance d'origine et choisissez Revoir et lancer.

 Important

Lancez une instance temporaire dans la même zone de disponibilité que l'instance d'origine. Si votre instance temporaire se trouve dans une zone de disponibilité différente, vous ne pouvez pas y attacher le volume racine de l'instance d'origine.

- d. Sur la page Review Instance Launch, sélectionnez Launch.
 - e. Lorsque vous y êtes invité, créez une nouvelle paire de clés, téléchargez-la dans un emplacement sûr de votre ordinateur, puis choisissez Lancer des instances.
2. Attachez le volume à l'instance temporaire en tant que volume secondaire, comme suit :
 - a. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume que vous avez détaché de l'instance d'origine, et sélectionnez Actions, Attacher un volume.
 - b. Dans la boîte de dialogue Attacher un volume, pour Instances, commencez par saisir le nom ou l'ID de votre instance temporaire, puis sélectionnez-la dans la liste.
 - c. Pour Appareil, saisissez **xvdf** (s'il n'est pas déjà présent), puis choisissez Attacher.

Étape 3 : Réinitialiser le mot de passe administrateur

Ensuite, connectez-vous à l'instance temporaire et utilisez EC2Launch pour réinitialiser le mot de passe administrateur.

Pour réinitialiser le mot de passe administrateur

1. Connectez-vous à l'instance temporaire et utilisez l'outil EC2Rescue for Windows Server sur l'instance pour réinitialiser le mot de passe administrateur comme suit :
 - a. Téléchargez le fichier .zip [EC2Rescue for Windows Server](#), extrayez le contenu et exécutez EC2Rescue.exe.
 - b. Sur l'écran License Agreement (Contrat de licence), lisez le contrat de licence et, si vous acceptez les conditions, choisissez I agree (J'accepte).
 - c. Sur l'écran Welcome to EC2Rescue for Windows Server, choisissez Next.
 - d. Sur l'écran Select mode, choisissez Offline instance.
 - e. Sur l'écran Select a disk, sélectionnez le périphérique xvdf et choisissez Next.
 - f. Confirmez la sélection de disque et choisissez Yes (Oui).
 - g. Une fois le volume chargé, choisissez OK.
 - h. Sur l'écran Select Offline Instance Option, choisissez Diagnose and Rescue.
 - i. Sur l'écran Summary, vérifiez les informations, puis choisissez Next.
 - j. Sur l'écran Detected possible issues, sélectionnez Reset Administrator Password et choisissez Next.
 - k. Sur l'écran Confirm, choisissez Rescue, OK.
 - l. Sur l'écran Done, choisissez Finish.
 - m. Fermez l'outil EC2Rescue for Windows Server, déconnectez-vous de l'instance temporaire, puis revenez à la console Amazon EC2.
2. Détachez le volume (xvdf) secondaire de l'instance temporaire comme suit :
 - a. Dans le panneau de navigation, sélectionnez Instances et choisissez l'instance temporaire.
 - b. Notez l'ID du volume EBS répertorié comme xvdf disponible sous l'onglet Stockage de l'instance temporaire.
 - c. Dans le panneau de navigation, choisissez Volumes.
 - d. Dans la liste des volumes, sélectionnez le volume noté à l'étape précédente, puis choisissez Actions et Détacher un volume. Une fois le statut du volume passé à disponible, passez à l'étape suivante.

Étape 4 : Redémarrer l'instance originale

Après avoir réinitialisé le mot de passe administrateur avec EC2Launch, rattachez le volume à l'instance originale en tant que volume racine et connectez-vous à l'instance en utilisant sa paire de clés pour récupérer le mot de passe administrateur.

Pour redémarrer l'instance originale

1. Rattachez le volume à l'instance originale comme suit :
 - a. Dans le panneau de navigation, choisissez Volumes, sélectionnez le volume que vous avez détaché de l'instance temporaire, et sélectionnez Actions, Attacher un volume.
 - b. Dans la boîte de dialogue Attacher un volume, pour Instances, saisissez le nom ou l'ID de votre instance d'origine, puis sélectionnez l'instance.
 - c. Pour Appareil, saisissez **/dev/sda1**.
 - d. Choisissez Attacher. Une fois le statut du volume passé à `in-use`, passez à l'étape suivante.
2. Dans le panneau de navigation, choisissez Instances. Sélectionnez l'instance d'origine et choisissez État de l'instance, Démarrer l'instance. Après que l'état de l'instance est passé à `Running`, passez à l'étape suivante.
3. Récupérez votre nouveau mot de passe administrateur Windows à l'aide de la clé privée de la nouvelle paire de clés et connectez-vous à l'instance. Pour de plus amples informations, veuillez consulter [Connexion à votre instance Windows](#).
4. (Facultatif) Vous pouvez résilier l'instance temporaire si vous n'en avez plus besoin. Sélectionnez l'instance temporaire, puis choisissez État de l'instance et Résilier l'instance.

Résolution d'un problème d'instance inaccessible

Vous pouvez utiliser les méthodes suivantes pour dépanner une instance Amazon EC2 inaccessible.

Table des matières

- [Redémarrage d'instance](#)
- [Sortie de la console de l'instance](#)
- [Création d'une capture d'écran d'une instance inaccessible](#)
- [Captures d'écran courantes pour les instances Windows](#)

- [Récupération d'instance en cas de plantage de l'ordinateur hôte](#)

Redémarrage d'instance

La capacité de redémarrer des instances qui sont généralement inaccessibles est précieuse pour le dépannage et la gestion générale des instances.

Tout comme vous pouvez réinitialiser un ordinateur en appuyant sur le bouton approprié, vous pouvez réinitialiser les instances EC2 en utilisant la console, l'interface ligne de commande ou l'API d'Amazon EC2. Pour plus d'informations, consultez [Redémarrer votre instance](#).

Sortie de la console de l'instance

La sortie de la console est un outil de valeur pour le diagnostic des problèmes. Elle est particulièrement utile pour la résolution des problèmes liés au noyau et à la configuration des services qui pourraient mettre fin à une instance ou la rendre inaccessible avant que son programme fantôme SSH ne puisse être démarré.

- Instances Linux : la sortie de la console d'instance affiche exactement la sortie de console qui serait normalement affichée sur un moniteur physique connecté à un ordinateur. La sortie de la console renvoie des informations mises en mémoire tampon qui ont été publiées après un état de transition d'instance (démarrage, arrêt, redémarrage et résiliation). La sortie publiée n'est pas continuellement mise à jour, uniquement lorsqu'elle est probablement très bénéfique.
- Instances Windows : le résultat de la console d'instance inclut les trois dernières erreurs du journal des événements du système.

Vous pouvez éventuellement extraire la dernière sortie de console série à tout moment au cours du cycle de vie de l'instance. Cette option n'est prise en charge que sur [les instances créées sur le système AWS Nitro](#). Elle n'est pas prise en charge via la console Amazon EC2.

Note

Seuls les 64 Ko les plus récents de la sortie publiée sont stockés et disponibles pendant au moins 1 heure après la dernière publication.

Seul le propriétaire de l'instance peut accéder à la sortie de la console.

Utilisez l'une des méthodes suivantes pour obtenir la sortie de la console.

Console

Pour obtenir la sortie de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, sélectionnez instances.
3. Sur la page Instances, sélectionnez Actions, Surveiller et dépanner, puis Obtenir le journal système.

Command line

Pour obtenir la sortie de la console

Vous pouvez utiliser l'une des commandes suivantes. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [get-console-output](#) (AWS CLI)
- [Get-EC2ConsoleOutput](#) (AWS Tools for Windows PowerShell)

Création d'une capture d'écran d'une instance inaccessible

Si vous ne parvenez pas à vous connecter à votre instance, vous pouvez en faire une capture d'écran et l'afficher sous forme d'image. Cette image permet de voir le statut de l'instance et de résoudre le problème plus rapidement.

Vous pouvez générer des captures d'écran pendant que l'instance s'exécute ou après son blocage. L'image est générée au format JPG et ne dépasse pas 100 Ko. Aucun coût de transfert de données n'est facturé pour la capture d'écran.

Limites

Cette fonctionnalité n'est pas prise en charge dans les cas suivants :

- Instances matériel nu (instances de type `*.metal`)
- L'instance utilise un pilote NVIDIA GRID
- [Instances alimentées par des processeurs Graviton basés sur ARM](#)

- Instances Windows activées AWS Outposts

Régions prises en charge

Cette fonction est disponible dans les régions suivantes :

- US East (N. Virginia) Region
- Région US East (Ohio)
- Région US West (N. California)
- Région US West (Oregon)
- Région Afrique (Le Cap)
- Région Asie-Pacifique (Hong Kong)
- Région Asie-Pacifique (Hyderabad)
- Région Asie-Pacifique (Jakarta)
- Région Asie-Pacifique (Melbourne)
- Région Asie-Pacifique (Mumbai)
- Région Asie-Pacifique (Osaka)
- Région Asie-Pacifique (Séoul)
- Région Asie-Pacifique (Singapour)
- Région Asie-Pacifique (Sydney)
- Région Asie-Pacifique (Tokyo)
- Région Canada (Centre)
- Région Canada Ouest (Calgary)
- Région Chine (Beijing)
- Région Chine (Ningxia)
- Région Europe (Frankfurt)
- Région Europe (Irlande)
- Région Europe (London)
- Europe (Milan) Region
- Région Europe (Paris)
- Région Europe (Espagne)
- Région Europe (Stockholm)

- Région Europe (Zurich)
- Région Israël (Tel Aviv)
- Région Amérique du Sud (São Paulo)
- Middle East (Bahrain) Region
- Région du Moyen-Orient (EAU)

Console

Obtention d'une capture d'écran d'une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, choisissez Instances.
3. Sélectionnez l'instance à capturer.
4. Sélectionnez Actions, Surveiller et dépanner puis Obtenir la capture d'écran d'instance.
5. Sélectionnez Télécharger ou cliquez avec le bouton droit sur l'image pour la télécharger et l'enregistrer.

Command line

Création d'une capture d'écran d'instance

Vous pouvez utiliser l'une des commandes suivantes. Le contenu renvoyé est codé en base64. Pour plus d'informations sur les CLI (interface ligne de commande), consultez [Accès à Amazon EC2](#).

- [get-console-screenshot](#) (AWS CLI)
- [GetConsoleCapture d'écran](#) (API de requête Amazon EC2)

Captures d'écran courantes pour les instances Windows

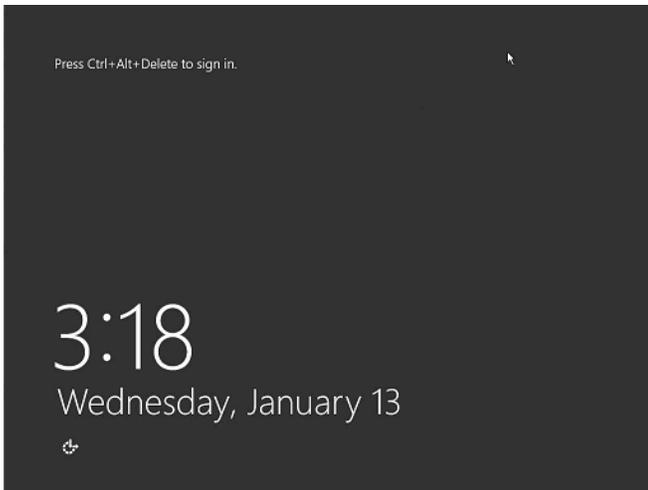
Aidez-vous des informations suivantes pour faciliter le dépannage d'une instance Windows inaccessible grâce aux captures d'écran renvoyées par le service.

- [Écran de connexion \(Ctrl+Alt+Suppr\)](#)
- [Écran de la console de récupération](#)
- [Écran du gestionnaire de démarrage Windows](#)

- [Écran Sysprep](#)
- [Écran de préparation](#)
- [Écran Windows Update](#)
- [Chkdsk](#)

Écran de connexion (Ctrl+Alt+Suppr)

Le service de capture d'écran de la console a renvoyé ce qui suit.



Si une instance devient inaccessible au cours de la connexion, le problème peut venir de votre configuration réseau ou des services Bureau à distance de Windows. Une instance peut également ne pas réagir si un processus utilise une quantité de mémoire important.

Configuration réseau

Utilisez les informations suivantes pour vérifier que votre configuration réseau AWS, celle de Microsoft Windows et celle de votre réseau local (ou local) ne bloquent pas l'accès à l'instance.

AWS configuration réseau

Configuration	Vérifier
Configuration du groupe de sécurité	Vérifiez que le port 3389 est ouvert pour votre groupe de sécurité. Vérifiez que vous vous connectez à l'adresse IP publique appropriée. Si l'instance n'a pas été associée à une EIP,

Configuration	Vérifier
	l'adresse IP publique change après l'arrêt ou le démarrage de l'instance. Pour plus d'informations, consultez Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant.
Configuration de VPC (ACL réseau)	Vérifiez que la liste de contrôle d'accès (ACL) de votre Amazon VPC ne bloque pas l'accès. Pour plus d'informations, consultez ACL réseau dans le Amazon VPC Guide de l'utilisateur.
Configuration VPN	Si vous vous connectez au VPC à l'aide d'un réseau privé virtuel (VPN), vérifiez la connectivité du tunnel VPN. Pour plus d'informations, consultez la page Comment résoudre les problèmes de connectivité des tunnels VPN au VPC Amazon ?

Configuration du réseau Windows

Configuration	Vérifier
Pare-feu Windows	Vérifiez que le pare-feu Windows ne bloque pas les connexions à votre instance. Désactivez le pare-feu Windows, comme décrit à l'étape 7 de la section de résolution des problèmes liés au service Bureau à distance, Le service Bureau à distance ne peut pas se connecter à l'ordinateur distant.
Configuration TCP/IP avancée (utilisation d'une adresse IP statique)	L'instance peut ne pas réagir si vous avez configuré une adresse IP statique. Pour un VPC, créez une interface réseau et attachez-la à l'instance.

Configuration réseau locale ou sur site

Vérifiez qu'une configuration réseau locale ne bloque pas l'accès. Essayez de vous connecter à une autre instance du même VPC comme l'instance inaccessible. Si vous ne parvenez pas à accéder à une autre instance, contactez votre administrateur de réseau local pour déterminer si une politique locale restreint l'accès.

Problème lié aux services Bureau à distance

Si l'instance n'est pas accessible lors de la connexion, le problème peut venir des services RDS sur l'instance.

Tip

Vous pouvez utiliser le runbook [AWSSupport-TroubleshootRDP](#) pour vérifier et modifier divers paramètres susceptibles d'affecter les connexions RDP (Remote Desktop Protocol). Pour plus d'informations, consultez [AWSSupport-TroubleshootRDP](#) dans la référence AWS Systems Manager Automation runbook.

Configuration des services Bureau à distance (RDS)

Configuration	Vérifier
Le service RDS est en cours d'exécution	Vérifiez que le service RDS est exécuté sur l'instance. Connectez-vous à l'instance via le composant logiciel enfichable Services (<code>services.msc</code>) de Microsoft Management Console (MMC). Dans la liste des services, vérifiez que Services Bureau à distance est défini sur En cours d'exécution. Si ce n'est pas le cas, démarrez-le, puis définissez le type de démarrage sur Automatique. Si vous ne parvenez pas à vous connecter à l'instance en utilisant le composant logiciel enfichable Services, détachez le volume racine de l'instance, créez un instantané ou une AMI du volume, attachez le volume d'origine à une autre instance dans la même zone de disponibilité en tant que volume secondaire et modifiez la clé de registre Start . Lorsque vous avez terminé, rattachiez le volume racine à l'instance d'origine.
Le service RDS est activé	Même si le service a été lancé, il peut être désactivé. Détachez le volume racine de l'instance, prenez un instantané du volume ou créez une AMI, attachez le volume d'origine à une autre

Configuration	Vérifier
	<p>instance dans la même zone de disponibilité en tant que volume secondaire, puis activez le service en modifiant la clé de registre Terminal Server comme décrit dans Activation du Bureau à distance sur une instance EC2 avec le Registre à distance.</p> <p>Lorsque vous avez terminé, rattachez le volume racine à l'instance d'origine.</p>

Utilisation élevée du processeur

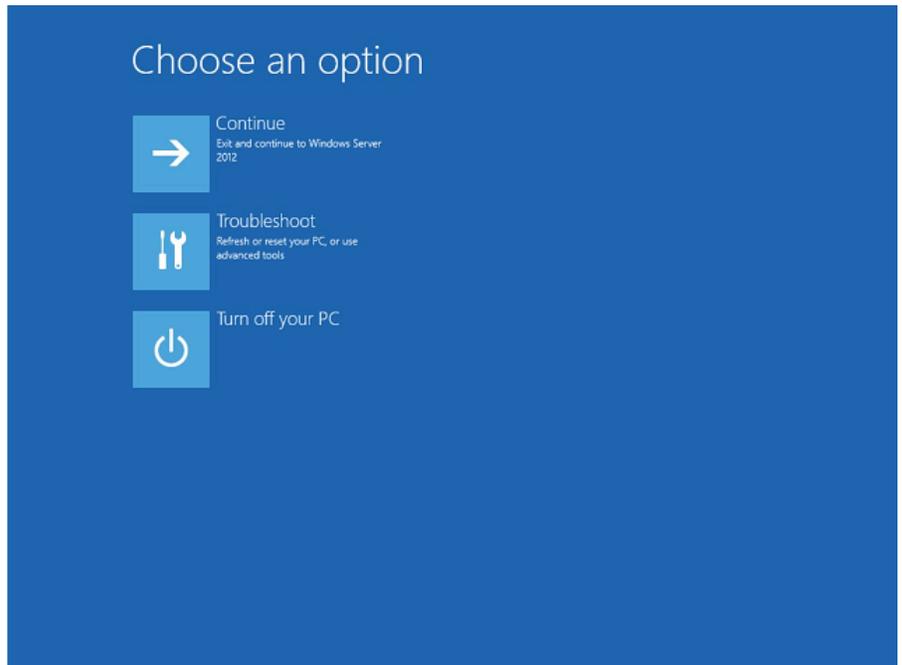
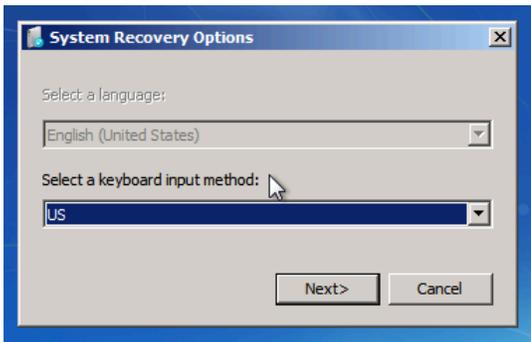
Vérifiez la métrique CPUUtilization (Maximum) sur votre instance à l'aide d'Amazon CloudWatch. Si la valeur CPUUtilization (Maximum) est élevée, attendez qu'elle baisse, puis essayez de vous reconnecter. Une utilisation élevée de l'UC a plusieurs origines possibles :

- Windows Update
- Analyse des logiciels de sécurité
- Script de démarrage personnalisé
- Planificateur de tâches

Pour plus d'informations, consultez [Obtenir des statistiques pour une ressource spécifique](#) dans le guide de CloudWatch l'utilisateur Amazon. Pour des conseils de dépannage supplémentaires, consultez la page [Utilisation élevée du processeur peu après le démarrage de Windows \(instances Windows uniquement\)](#).

Écran de la console de récupération

Le service de capture d'écran de la console a renvoyé ce qui suit.



Le système d'exploitation peut démarrer dans la console de récupération et rester bloqué dans cet état si la stratégie `bootstatuspolicy` n'est pas définie sur `ignoreallfailures`. Utilisez la procédure suivante pour remplacer la configuration `bootstatuspolicy` par `ignoreallfailures`.

Par défaut, la configuration des politiques pour les AMI Windows publiques fournies par AWS est définie sur `ignoreallfailures`.

1. Arrêtez l'instance inaccessible.
2. Créez un instantané du volume racine. Le volume racine est attaché à l'instance en tant que `/dev/sda1`.

Détachez le volume racine de l'instance inaccessible, créez un instantané ou une AMI du volume et attachez-le à une autre instance dans la même zone de disponibilité en tant que volume secondaire.

Warning

Si votre instance temporaire et l'instance d'origine sont lancées grâce à la même AMI, vous devez effectuer des étapes supplémentaires ou vous ne pourrez pas démarrer l'instance d'origine après la restauration de son volume racine en raison d'une collision de signature de disque. Si vous devez créer une instance temporaire à l'aide de la même AMI pour éviter une collision de signature de disque, complétez les étapes en [Collision de signature de disque](#).

Sinon, sélectionnez une autre AMI pour l'instance temporaire. Par exemple, si l'instance d'origine utilise une AMI pour Windows Server 2016, lancez l'instance temporaire à l'aide d'une AMI pour Windows Server 2019.

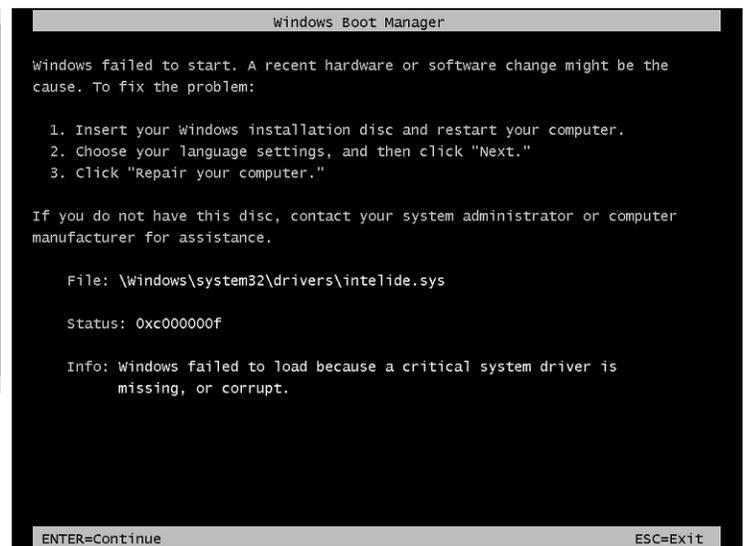
3. Connectez-vous à l'instance et exécutez la commande suivante à partir d'une invite de commande pour remplacer la configuration `bootstatuspolicy` par `ignoreallfailures`.

```
bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy ignoreallfailures
```

4. Rattachez le volume à l'instance inaccessible et redémarrez cette dernière.

Écran du gestionnaire de démarrage Windows

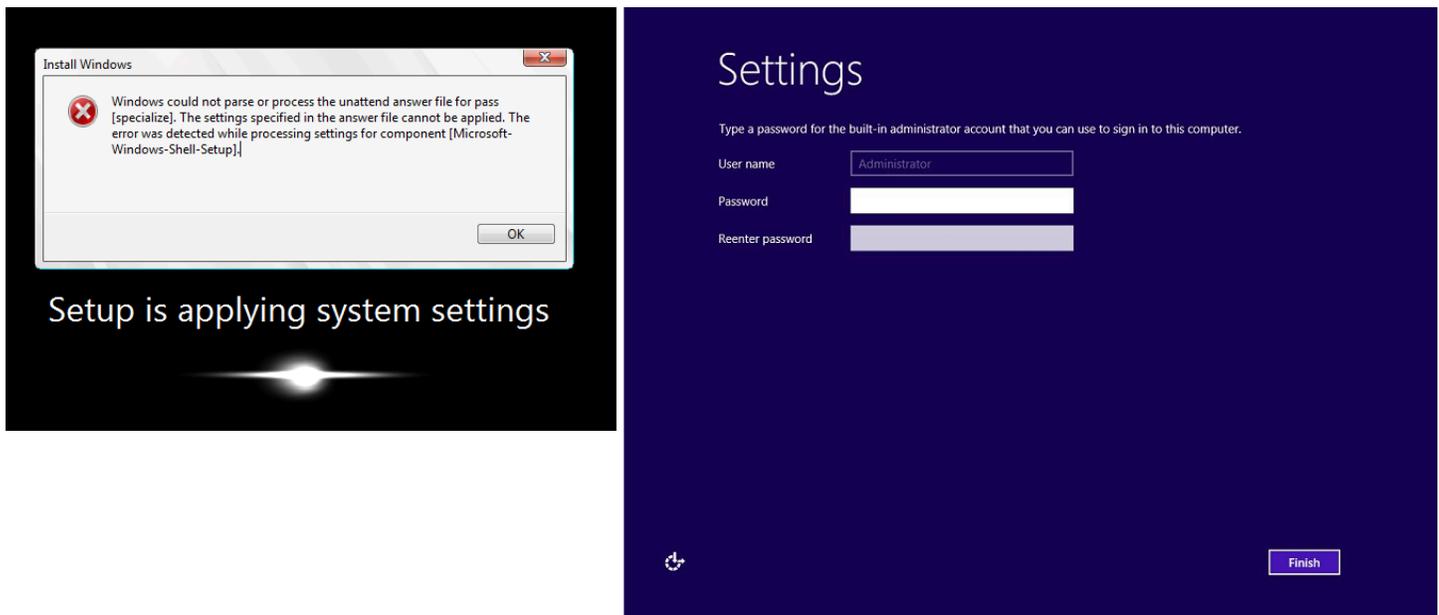
Le service de capture d'écran de la console a renvoyé ce qui suit.



Le système d'exploitation a subi une corruption irréversible dans le système de fichier et/ou le registre. Lorsque l'instance est bloquée dans cet état, vous devez récupérer l'instance à partir d'une AMI de sauvegarde récente ou lancer une instance de remplacement. Si vous devez accéder aux données de l'instance, détachez les volumes racines de l'instance inaccessible, créez un instantané ou une AMI de ces volumes et attachez-les à une autre instance dans la même zone de disponibilité en tant que volume secondaire.

Écran Sysprep

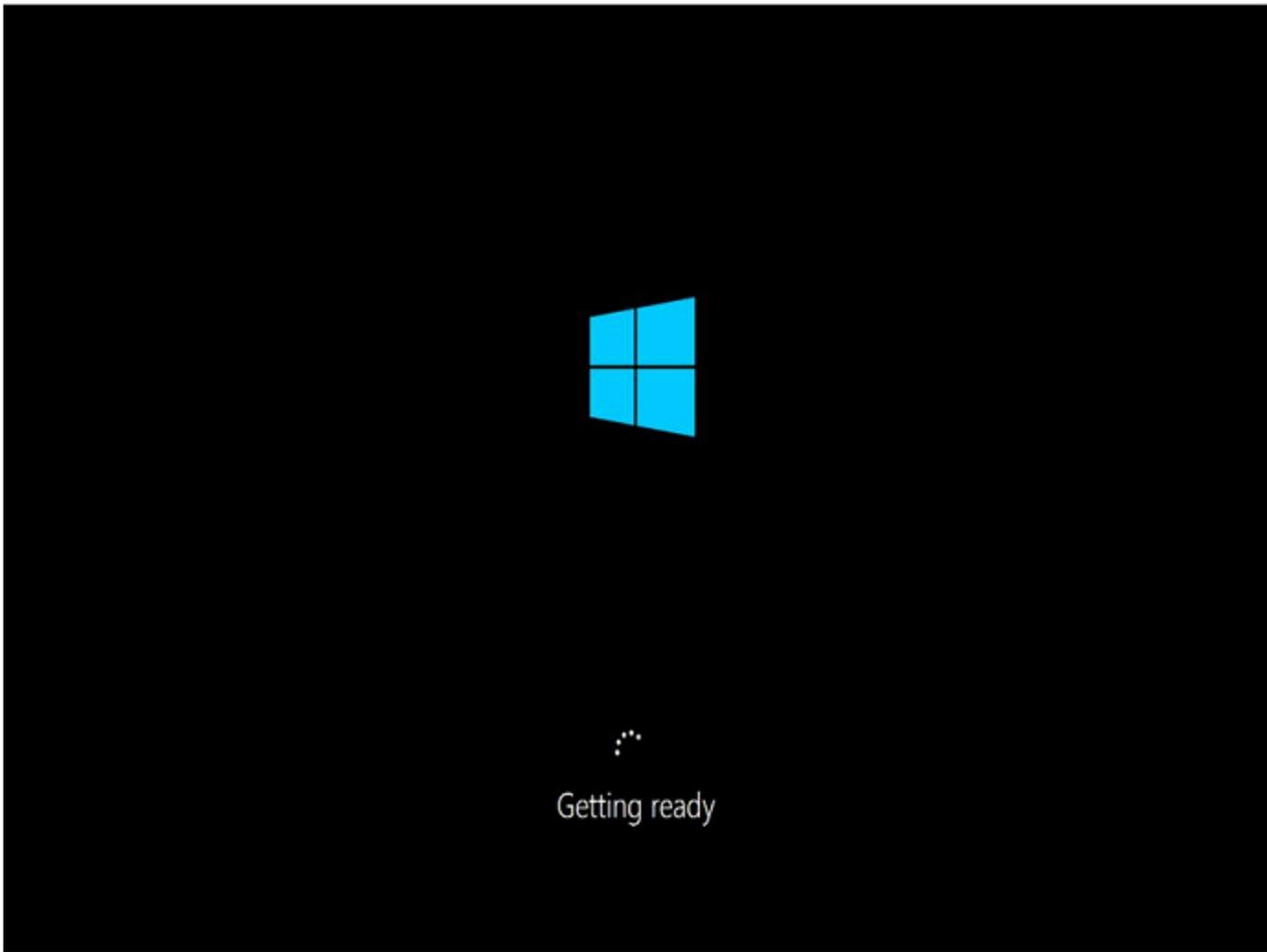
Le service de capture d'écran de la console a renvoyé ce qui suit.



Vous voyez cet écran si vous n'avez pas utilisé le service EC2Config pour appeler Sysprep ou si le système d'exploitation a échoué lors de l'exécution de Sysprep. Vous pouvez réinitialiser le mot de passe à l'aide [EC2Rescue](#). Sinon, consultez [Création d'une AMI avec Windows Sysprep](#).

Écran de préparation

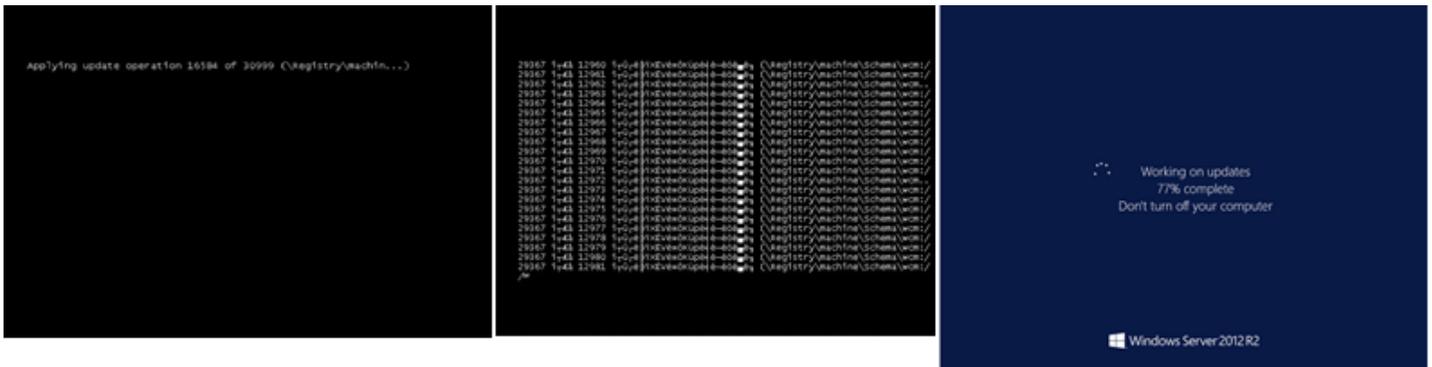
Le service de capture d'écran de la console a renvoyé ce qui suit.



Actualisez le service de capture d'écran de la console d'instance plusieurs fois pour vérifier que l'anneau de progression tourne. Si l'anneau tourne, attendez que le système d'exploitation démarre. Vous pouvez également vérifier la métrique CPUUtilization (Maximum) sur votre instance en utilisant Amazon CloudWatch pour vérifier si le système d'exploitation est actif. Si l'anneau de progression ne tourne pas, l'instance est peut-être bloquée au niveau du processus de démarrage. Redémarrez l'instance. Si le redémarrage ne résout pas le problème, récupérez l'instance à partir d'une AMI de sauvegarde récente ou lancez une instance de remplacement. Si vous avez besoin d'accéder aux données de l'instance, détachez le volume racine de l'instance inaccessible et créez un instantané ou une AMI du volume. Attachez-le ensuite à une autre instance de la même zone de disponibilité en tant que volume secondaire.

Écran Windows Update

Le service de capture d'écran de la console a renvoyé ce qui suit.



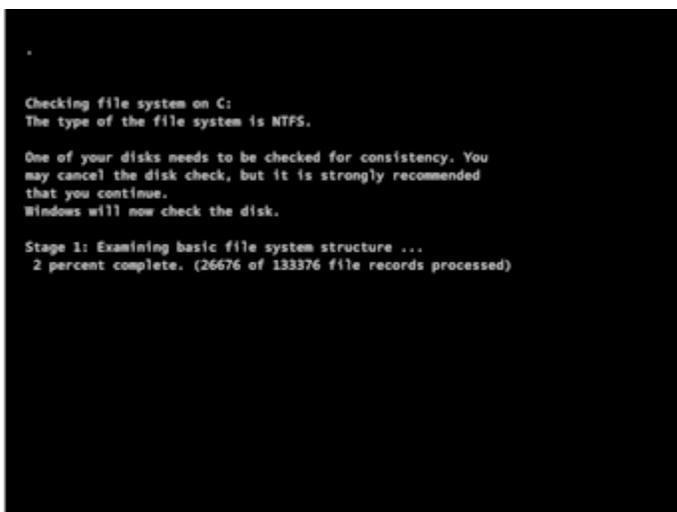
Le processus Windows Update met à jour le registre. Attendez que la mise à jour soit terminée. Ne redémarrez ou n'arrêtez pas l'instance, car cela peut entraîner une corruption des données au cours de la mise à jour.

Note

Le processus Windows Update peut utiliser des ressources sur le serveur au cours de la mise à jour. Si vous rencontrez souvent ce problème, pensez à utiliser des types d'instance et des volumes EBS plus rapides.

Chkdsk

Le service de capture d'écran de la console a renvoyé ce qui suit.



Windows exécute l'outil système chkdsk sur le disque pour vérifier l'intégrité du système de fichiers et pour corriger les erreurs système des fichiers logiques. Attendez que le processus se termine.

Récupération d'instance en cas de plantage de l'ordinateur hôte

S'il existe un problème irrécupérable lié au matériel d'un ordinateur hôte sous-jacent, AWS peut planifier un événement d'arrêt d'instance. Vous êtes averti d'un tel événement en avance par e-mail.

Pour récupérer une instance basée sur Amazon EBS en cours d'exécution sur un ordinateur hôte qui a planté

1. Sauvegardez les données importantes qui se trouvent sur les volumes de stockage d'instance sur Amazon EBS ou Amazon S3.
2. Arrêtez l'instance.
3. Démarrez l'instance.
4. Restaurez toutes les données importantes.

Pour plus d'informations, consultez [Arrêtez et démarrez les instances Amazon EC2](#).

Pour récupérer une instance basée sur le stockage d'instance et exécutée sur un ordinateur hôte qui a planté

1. Créez une AMI à partir de l'instance.
2. Chargez l'image vers Amazon S3.
3. Sauvegardez les données importantes sur Amazon EBS ou Amazon S3.
4. Mettez fin à l'instance.
5. Lancez une nouvelle instance depuis l'AMI.
6. Restaurez toutes les données importantes sur la nouvelle instance.

Résoudre les problèmes d'arrêt de votre instance

Si vous avez arrêté votre instance basée sur Amazon EBS et que celle-ci semble « bloquée » à l'état `stopping`, il peut y avoir un problème avec l'ordinateur hôte sous-jacent.

L'utilisation d'une instance est gratuite tant que l'instance est à l'état `stopping` ou à n'importe quel autre état, sauf `running`. L'utilisation d'une instance est payante uniquement lorsqu'elle est à l'état `running`.

Forcer l'arrêt de l'instance

Forcez l'arrêt de l'instance à l'aide de la console ou de l'AWS CLI.

Note

Vous pouvez forcer une instance à cesser d'utiliser la console uniquement lorsque l'instance est dans l'état `stopping`. Vous pouvez forcer une instance à cesser d'utiliser la AWS CLI lorsque l'instance est dans n'importe quel état, sauf `shutting-down` et `terminated`.

Console

Pour forcer l'arrêt de l'instance à l'aide de la console

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez instances et choisissez l'instance bloquée.
3. Sélectionnez État de l'instance, Forcer l'arrêt de l'instance, Arrêter.

Notez que Forcer l'arrêt de l'instance n'est disponible dans la console que si votre instance se trouve dans l'état `stopping`. Si votre instance est dans un autre état (sauf `shutting-down` et `terminated`), vous pouvez utiliser le AWS CLI pour forcer l'arrêt de votre instance.

AWS CLI

Pour forcer l'arrêt de l'instance à l'aide du AWS CLI

Utilisez la commande [stop-instances](#) et l'option `--force` comme suit :

```
aws ec2 stop-instances --instance-ids i-0123ab456c789d01e --force
```

Si l'instance ne s'est pas arrêtée après 10 minutes, publiez une demande d'aide sur le [AWS re:Post](#). Pour contribuer à une résolution rapide du problème, incluez l'ID d'instance et décrivez les étapes que vous avez déjà effectuées. Sinon, si vous disposez d'un plan de support, créez une demande d'assistance technique dans le [Centre de support](#).

Créer une instance de remplacement

Pour essayer de résoudre le problème en attendant d'obtenir de l'aide de la part du [AWS re:Post](#) ou du [Centre de support](#), créez une instance de remplacement. Créez une AMI de l'instance bloquée et lancez une nouvelle instance à l'aide de cette AMI.

Important

La création d'une instance de remplacement est recommandée si elle enregistre uniquement [des contrôles d'état du système](#), car les contrôles d'état des instances obligeront l'AMI à copier un réplica exact du système d'exploitation en panne. Une fois que vous avez confirmé le message d'état, créez l'AMI et lancez une nouvelle instance à l'aide de cette AMI.

Console

Pour créer une instance de remplacement à l'aide de la console

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez instances et choisissez l'instance bloquée.
3. Choisissez Actions, Image and templates (Image et modèles), Create image (Créer une image).
4. Sur la page Créer une image, procédez comme suit :
 - a. Saisissez un nom et une description pour l'AMI.
 - b. Sélectionnez Pas de redémarrage.
 - c. Choisissez Create image (Créer une image).

Pour plus d'informations, consultez [the section called "Création d'une AMI à partir d'une instance"](#).

5. Lancez une nouvelle instance à partir de l'AMI et vérifiez qu'elle fonctionne.
6. Sélectionnez l'instance bloquée, puis Actions, État de l'instance et Résilier l'instance. Si l'instance reste également bloquée lors de la mise hors service, Amazon EC2 force automatiquement sa mise hors service en quelques heures.

AWS CLI

Pour créer une instance de remplacement à l'aide de la CLI

1. Créez une AMI à partir de l'instance bloquée, en utilisant la commande [create-image](#) (AWS CLI) et l'option `--no-reboot` de la façon suivante .

```
aws ec2 create-image --instance-id i-0123ab456c789d01e --name "AMI" --  
description "AMI for replacement instance" --no-reboot
```

2. Lancez une nouvelle instance à partir de l'AMI en utilisant la commande [run-instances](#) (AWS CLI) de la façon suivante :

```
aws ec2 run-instances --image-id ami-1a2b3c4d --count 1 --instance-type c3.large  
--key-name MyKeyPair --security-groups MySecurityGroup
```

3. Vérifiez que la nouvelle instance fonctionne.
4. Mettez fin à l'instance bloquée en utilisant la commande [terminate-instances](#) (AWS CLI) de la façon suivante :

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

Si vous ne pouvez pas créer une AMI à partir de l'instance comme décrit dans la procédure précédente, vous pouvez configurer une instance de remplacement de la façon suivante :

(Alternative) Pour créer une instance de remplacement à l'aide de la console

1. Sélectionnez l'instance et choisissez Description, Périphériques de stockage en mode bloc. Sélectionnez chaque volume et notez leur ID de volume. Assurez-vous de noter quel volume correspond au volume racine.
2. Dans le panneau de navigation, choisissez Volumes. Sélectionnez chaque volume pour l'instance et sélectionnez Actions, Créer un instantané.
3. Dans le panneau de navigation, choisissez Snapshots. Sélectionnez l'instantané que vous venez de créer et choisissez Actions, Créer un volume.
4. Lancez une instance avec le même système d'exploitation que l'instance bloqué. Notez l'ID du volume et le nom de périphérique de son volume racine.

5. Dans le panneau de navigation, sélectionnez instances, puis l'instance que vous venez de lancer, et État de l'instance, Arrêter l'instance.
6. Dans le panneau de navigation, sélectionnez Volumes, choisissez le volume racine de l'instance arrêtée, et sélectionnez Actions, Détacher un volume.
7. Sélectionnez le volume racine que vous avez créé à partir de l'instance bloquée, puis Actions, Attacher un volume et attachez-le à la nouvelle instance comme volume racine (en utilisant le nom de périphérique que vous avez noté). Attachez n'importe quel volume non-racine supplémentaire à l'instance.
8. Dans le panneau de navigation, sélectionnez instances et choisissez l'instance de remplacement. Choisissez État de l'instance, Démarrer l'instance. Vérifiez que l'instance fonctionne.
9. Sélectionnez l'instance bloquée, choisissez État de l'instance, Résilier l'instance. Si l'instance reste également bloquée lors de la mise hors service, Amazon EC2 force automatiquement sa mise hors service en quelques heures.

Résoudre les problèmes de résiliation d'instance (arrêt)

Vous n'êtes pas facturé pour l'utilisation d'une instance tant que l'instance n'est pas à l'état `running`. En d'autres termes, lorsque vous mettez fin à une instance, l'instance ne vous est plus facturée dès que son état passe à `shutting-down`.

Mise hors service immédiate de l'instance

Plusieurs problèmes peuvent entraîner la résiliation immédiate de votre instance au démarrage. Pour plus d'informations, consultez [Mise hors service immédiate de l'instance](#).

Mise à fin d'instance retardée

Si votre instance reste à l'état `shutting-down` pendant plus que quelques minutes, elle peut être retardée à cause des scripts d'arrêt exécutés par l'instance.

Un autre cause possible est un problème avec l'ordinateur hôte sous-jacent. Si votre instance reste à l'état `shutting-down` pendant plusieurs heures, Amazon EC2 la considère comme une instance bloquée et la résilie de force.

S'il semble que votre instance soit bloquée pendant la mise à fin et que cela dure depuis plus de quelques heures, envoyez une demande d'aide à [AWS re:Post](#). Pour aider à accélérer la résolution

d'un problème, incluez l'ID d'instance et décrivez les étapes que vous avez déjà effectuées. Sinon, si vous disposez d'un plan de support, créez une demande d'assistance technique dans le [Centre de support](#).

Instance terminée toujours affichée

Après avoir mis fin à une instance, elle reste visible pendant un court instant avant d'être supprimée. L'état indique `terminated`. Si l'entrée n'est pas supprimée après plusieurs heures, contactez le support.

Erreur : il se peut que l'instance ne soit pas résiliée. Modifier son attribut d'instance « désactiver `ApiTermination` »

Si vous essayez de résilier une instance et que le message d'erreur `The instance instance_id may not be terminated. Modify its 'disableApiTermination' instance attribute` s'affiche, cela signifie que la protection contre la résiliation de l'instance a été activée. La protection contre la résiliation empêche la résiliation accidentelle de l'instance. Pour plus d'informations, consultez [Activer la protection de la résiliation](#).

Vous devez désactiver la protection contre la résiliation avant de pouvoir résilier l'instance.

Pour désactiver la protection contre la résiliation à l'aide de la console Amazon EC2, sélectionnez l'instance, puis choisissez Actions, Paramètres de l'instance, Modifier la protection contre la résiliation.

Pour désactiver la protection contre le licenciement à l'aide de AWS CLI, utilisez la commande suivante.

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-disable-api-termination
```

instances lancées ou terminées automatiquement

De manière générale, ces comportements signifient que vous avez utilisé Amazon EC2 Auto Scaling, la flotte EC2 ou le parc d'instances Spot pour mettre automatiquement à l'échelle vos ressources de calcul en fonction des critères que vous avez définis.

- Vous mettez fin à une instance et une nouvelle instance se lance automatiquement.
- Vous lancez une instance et l'une de vos instances se termine automatiquement.

- Vous arrêtez une instance, elle se termine et une nouvelle instance se lance automatiquement.

Pour arrêter la scalabilité automatique, consultez [Amazon EC2 Auto Scaling Guide de l'utilisateur](#), [EC2 Fleet](#), ou [Créer une Spot Fleet request](#).

Résoudre les problèmes des instances Linux dont les vérifications d'état ont échoué

Note

Cette rubrique s'applique uniquement aux instances Linux.

Les informations suivantes peuvent vous aider à résoudre les problèmes si la vérification de statut de votre instance Linux échoue. Commencez par déterminer si vos applications présentent des problèmes. Si vous constatez que l'instance n'exécute pas vos applications comme prévu, passez en revue les informations de contrôle de statut et les journaux système.

Pour des exemples de problèmes pouvant entraîner l'échec des vérifications d'état, consultez [Contrôles de statut pour vos instances](#).

Sommaire

- [Examen des informations de contrôle de statut](#)
- [Récupération des journaux système](#)
- [Résoudre les erreurs du journal système pour les instances Linux](#)
- [Mémoire insuffisante : processus d'arrêt](#)
- [ERROR: mmu_update failed \(la mise à jour de la gestion de la mémoire a échoué\)](#)
- [Erreur d'E/S \(échec du périphérique de stockage en mode bloc\)](#)
- [I/O ERROR: neither local nor remote disk \(le périphérique de stockage en mode bloc distribué ne fonctionne plus\)](#)
- [request_module: runaway loop modprobe \(modprobe en boucle sur le noyau hérité sur des versions Linux plus anciennes\)](#)
- [« FATAL: kernel too old » et « fsck: No such file or directory while trying to open /dev » \(décalage entre le noyau et l'AMI\)](#)
- [« FATAL : Impossible de charger /lib/modules » ou « BusyBox » \(modules de noyau manquants\)](#)

- [ERROR Invalid kernel \(noyau incompatible EC2\)](#)
- [fsck : aucun fichier ou répertoire de ce type lors de la tentative d'ouverture... \(système de fichiers non trouvé\)](#)
- [General error mounting filesystems \(Montage en échec\)](#)
- [VFS: Unable to mount root fs on unknown-block \(le système de fichiers racine ne correspond pas\)](#)
- [Erreur : Unable to determine major/minor number of root device... \(décalage du système de fichiers/périphérique racine\)](#)
- [XENBUS : Device with no driver...](#)
- [... days without being checked, check forced \(Contrôle du système de fichiers nécessaire\)](#)
- [fsck a échoué à l'état de sortie... \(périphérique manquant\)](#)
- [Invite GRUB \(grubdom>\)](#)
- [Mise en service de l'interface eth0 : l'adresse MAC du périphérique eth0 est différente de celle attendue, ignorer. \(Adresse MAC codée de manière irréversible\)](#)
- [Impossible de charger la politique SELinux. L'appareil est en mode d'exécution. Arrêt maintenant. \(Erreur de configuration SELinux\)](#)
- [XENBUS: Timeout connecting to devices \(délai d'attente Xenbus\)](#)

Examen des informations de contrôle de statut

Pour enquêter sur les instances dégradées en utilisant la console Amazon EC2

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez instances, puis sélectionnez votre instance.
3. Dans le volet des détails, sélectionnez Statuts et alarmes pour voir les résultats individuels pour tous les Contrôles de statut de système et Contrôles de statut des instances.

Si un contrôle de statut d'un système a échoué, vous pouvez essayer l'une des options suivantes :

- Créez une alarme de récupération d'instance. Pour plus d'informations, consultez [Créer des alarmes qui arrêtent, finissent, redémarrent ou récupèrent une instance](#).
- Si vous avez changé le type d'instance pour une [instance basée sur le système AWS Nitro](#), les vérifications d'état échouent si vous avez migré depuis une instance qui ne possède pas les pilotes ENA et NVMe requis. Pour plus d'informations, consultez [Compatibilité pour modifier le type d'instance](#).

- Pour une instance qui utilise une AMI basée sur des volumes Amazon EBS, arrêtez et relancez l'instance.
- Pour une instance qui utilise une AMI basée sur le stockage d'instance, arrêtez l'instance et lancez-en une autre.
- Attendez qu'Amazon EC2 résolve le problème.
- Publiez votre problème sur [AWS re:Post](#).
- Si votre instance est dans un groupe Auto Scaling, le service Amazon EC2 Auto Scaling lance automatiquement une instance de remplacement. Pour plus d'informations, consultez [Vérification de l'état des instances Auto Scaling](#) dans le Amazon EC2 Auto Scaling Guide de l'utilisateur.
- Récupérez le journal du système et recherchez les erreurs.

Récupération des journaux système

Si un contrôle de statut d'instance échoue, vous pouvez relancer l'instance et récupérer les journaux du système. Les journaux peuvent révéler une erreur que peut vous aider à résoudre le problème. Le redémarrage efface les informations inutiles des journaux.

Pour redémarrer une instance et récupérer le journal du système

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez instances, puis choisissez votre instance.
3. Sélectionnez État de l'instance, puis Redémarrer l'instance. Le redémarrage de votre instance peut prendre quelques minutes.
4. Vérifiez si le problème existe encore. Dans certains cas, le redémarrage peut résoudre le problème.
5. Lorsque l'état de l'instance est `running`, sélectionnez Actions, Surveiller et dépanner, Obtenir le journal système.
6. Consultez le journal qui apparaît à l'écran et utilisez la liste ci-dessous des déclarations d'erreurs connues du journal du système afin de résoudre votre problème.
7. Si votre problème n'est pas résolu, vous pouvez le publier sur [AWS re:Post](#).

Résoudre les erreurs du journal système pour les instances Linux

Pour les instances Linux qui ont échoué à une vérification de l'état de l'instance, telle que la vérification de l'accessibilité de l'instance, vérifiez que vous avez suivi les étapes ci-dessus

pour récupérer le journal système. La liste suivante contient certaines erreurs communes du journal du système et les actions suggérées que vous pouvez prendre pour résoudre le problème correspondant à chaque erreur.

Memory Errors

- [Mémoire insuffisante : processus d'arrêt](#)
- [ERROR: mmu_update failed \(la mise à jour de la gestion de la mémoire a échoué\)](#)

Device Errors

- [Erreur d'E/S \(échec du périphérique de stockage en mode bloc\)](#)
- [I/O ERROR: neither local nor remote disk \(le périphérique de stockage en mode bloc distribué ne fonctionne plus\)](#)

Kernel Errors

- [request_module: runaway loop modprobe \(modprobe en boucle sur le noyau hérité sur des versions Linux plus anciennes\)](#)
- [« FATAL: kernel too old » et « fsck: No such file or directory while trying to open /dev » \(décalage entre le noyau et l'AMI\)](#)
- [« FATAL : Impossible de charger /lib/modules » ou « BusyBox » \(modules de noyau manquants\)](#)
- [ERROR Invalid kernel \(noyau incompatible EC2\)](#)

File System Errors

- [fsck : aucun fichier ou répertoire de ce type lors de la tentative d'ouverture... \(système de fichiers non trouvé\)](#)
- [General error mounting filesystems \(Montage en échec\)](#)
- [VFS: Unable to mount root fs on unknown-block \(le système de fichiers racine ne correspond pas\)](#)
- [Erreur : Unable to determine major/minor number of root device... \(décalage du système de fichiers/périphérique racine\)](#)
- [XENBUS : Device with no driver...](#)
- [... days without being checked, check forced \(Contrôle du système de fichiers nécessaire\)](#)
- [fsck a échoué à l'état de sortie... \(périphérique manquant\)](#)

Operating System Errors

- [Invite GRUB \(grubdom>\)](#)
- [Mise en service de l'interface eth0 : l'adresse MAC du périphérique eth0 est différente de celle attendue, ignorer. \(Adresse MAC codée de manière irréversible\)](#)
- [Impossible de charger la politique SELinux. L'appareil est en mode d'exécution. Arrêt maintenant. \(Erreur de configuration SELinux\)](#)
- [XENBUS: Timeout connecting to devices \(délai d'attente Xenbus\)](#)

Mémoire insuffisante : processus d'arrêt

Une out-of-memory erreur est indiquée par une entrée du journal système similaire à celle illustrée ci-dessous.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879  
or a child  
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-  
rss:101196kB, file-rss:204kB
```

Cause potentielle

Mémoire épuisée

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Effectuez l'une des actions suivantes : <ul style="list-style-type: none">• Arrêtez l'instance et modifiez l'instance pour utiliser un type d'instance différent, puis relancez l'instance. Par exemple, un type d'instance plus importante ou optimisée pour la mémoire.• Redémarrez l'instance pour la renvoyer vers un statut non-défaillant. Le problème se

Pour ce type d'instance	Faire ceci
	reproduira probablement à moins que vous ne changiez de type d'instance.
Basée sur le stockage d'instance	Effectuez l'une des actions suivantes : <ul style="list-style-type: none">• Arrêtez l'instance et lancez une nouvelle instance en spécifiant un type d'instance différent. Par exemple, un type d'instance plus importante ou optimisée pour la mémoire.• Redémarrez l'instance pour la renvoyer vers un statut non-défaillant. Le problème se reproduira probablement à moins que vous ne changiez de type d'instance.

ERROR: mmu_update failed (la mise à jour de la gestion de la mémoire a échoué)

Les échecs de la mise à jour de la gestion de la mémoire sont indiqués par une entrée du journal du système qui est similaire à ce qui suit :

```
...
Press `ESC' to enter the menu... 0 [H[J Booting 'Amazon Linux 2011.09
(2.6.35.14-95.38.amzn1.i686)'

root (hd0)

Filesystem type is ext2fs, using whole disk

kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=
en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

Cause potentielle

Problème avec Amazon Linux

Action suggérée

Publiez votre problème sur [Forums dédiés aux développeurs](#) ou contactez [AWS Support](#).

Erreur d'E/S (échec du périphérique de stockage en mode bloc)

Une erreur d'entrée/sortie est indiquée par une entrée du journal du système qui est similaire à l'exemple suivant :

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

Causes potentielles

Type d'instance	Cause potentielle
Basée sur Amazon EBS	Un volume Amazon EBS en échec
Basée sur le stockage d'instance	Un lecteur physique en échec

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	<p>Utilisez la procédure suivante.</p> <ol style="list-style-type: none">1. Arrêtez l'instance.2. Dissociez le volume.3. Essayez de récupérer le volume. <div data-bbox="867 611 1507 972"><p> Note</p><p>Il est recommandé de faire souvent des instantanés de vos volumes Amazon EBS. Cela diminue considérablement le risque de perte de données suite à un échec.</p></div> <ol style="list-style-type: none">4. Attachez de nouveau le volume à l'instance.5. Démarrez l'instance.
Basée sur le stockage d'instance	<p>Mettez fin à l'instance et lancez une nouvelle instance.</p> <div data-bbox="829 1251 1507 1520"><p> Note</p><p>Les données ne peuvent pas être récupérées. Récupérez-les grâce aux sauvegardes.</p></div> <div data-bbox="829 1583 1507 1860"><p> Note</p><p>Il est recommandé d'utiliser soit Amazon S3, soit Amazon EBS pour les sauvegardes. Les volumes de stockage d'instance sont directement reliés</p></div>

Pour ce type d'instance	Faire ceci
	aux échecs d'un hôte et d'un disque uniques.

I/O ERROR: neither local nor remote disk (le périphérique de stockage en mode bloc distribué ne fonctionne plus)

Une erreur d'entrée/sortie sur le périphérique est indiquée par une entrée du journal du système qui est similaire à l'exemple suivant :

```
...
block drbd1: Local I/O failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: I/O ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

Causes potentielles

Type d'instance	Cause potentielle
Basée sur Amazon EBS	Un volume Amazon EBS en échec
Basée sur le stockage d'instance	Un lecteur physique en échec

Action suggérée

Mettez fin à l'instance et lancez une nouvelle instance.

Pour une instance basée sur Amazon EBS, vous pouvez récupérer des données à partir d'un instantané récent en créant une image à partir de celle-ci. Toutes les données ajoutées après l'instantané ne peuvent pas être récupérées.

request_module: runaway loop modprobe (modprobe en boucle sur le noyau hérité sur des versions Linux plus anciennes)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous. L'utilisation d'un noyau Linux instable ou ancien (par exemple, 2.6.16-xenU) peut entraîner une condition de boucle interminable au démarrage.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
```

```
BIOS-provided physical RAM map:
```

```
Xen: 0000000000000000 - 0000000026700000 (usable)
```

```
0MB HIGHMEM available.
```

```
...
```

```
request_module: runaway loop modprobe binfmt-464c
```

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Utilisez un noyau plus récent, soit basé sur GRUB ou statique, avec l'une des options suivantes:

Pour ce type d'instance	Faire ceci
	<p>Option 1 : Arrêtez l'instance et lancez une nouvelle instance en spécifiant les paramètres <code>-kernel</code> et <code>-ramdisk</code>.</p> <p>Option 2 :</p> <ol style="list-style-type: none"> 1. Arrêtez l'instance. 2. Modifiez les attributs de noyau et de ramdisk pour utiliser un noyau plus récent. 3. Démarrez l'instance.
Basée sur le stockage d'instance	Arrêtez l'instance et lancez une nouvelle instance en spécifiant les paramètres <code>-kernel</code> et <code>-ramdisk</code> .

« FATAL: kernel too old » et « fsck: No such file or directory while trying to open /dev » (décalage entre le noyau et l'AMI)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

Causes potentielles

Noyau et identifiant incompatibles

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Utilisez la procédure suivante.

Pour ce type d'instance	Faire ceci
	<ol style="list-style-type: none">1. Arrêtez l'instance.2. Modifiez la configuration pour utiliser un noyau plus récent.3. Démarrez l'instance.
Basée sur le stockage d'instance	Utilisez la procédure suivante. <ol style="list-style-type: none">1. Créez une AMI qui utilise un noyau plus récent.2. Mettez fin à l'instance.3. Démarrez une nouvelle instance à partir de l'AMI que vous avez créée.

« FATAL : Impossible de charger /lib/modules » ou « BusyBox » (modules de noyau manquants)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
[ 0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or
directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No
such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
directory
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
```

```
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device. Common problems:
- Boot args (cat /proc/cmdline)
- Check rootdelay= (did the system wait long enough?)
- Check root= (did the system wait for the right device?)
- Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!

BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

Causes potentielles

Une ou plusieurs conditions suivantes peuvent entraîner ce problème :

- Ramdisk manquant
- Modules corrects manquants pour le ramdisk
- Le volume racine Amazon EBS n'est pas attaché correctement en tant que /dev/sda1

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Utilisez la procédure suivante. <ol style="list-style-type: none">1. Sélectionnez ramdisk corrigé pour le volume Amazon EBS.2. Arrêtez l'instance.3. Détachez le volume et réparez-le.

Pour ce type d'instance	Faire ceci
	<ol style="list-style-type: none">4. Attachez le volume à l'instance.5. Démarrez l'instance.6. Modifiez l'AMI pour utiliser le ramdisk corrigé.
Basée sur le stockage d'instance	<p>Utilisez la procédure suivante.</p> <ol style="list-style-type: none">1. Arrêtez l'instance et lancez une nouvelle instance avec le bon ramdisk.2. Créez une nouvelle AMI avec le bon ramdisk.

ERROR Invalid kernel (noyau incompatible EC2)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
...
root (hd0)

Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

Booting 'Fallback'

root (hd0)

Filesystem type is ext2fs, using whole disk
```

```
kernel /vmlinuz.old root=/dev/sda1 ro
```

```
Error 15: File not found
```

Causes potentielles

Une ou deux des conditions suivantes peuvent entraîner ce problème :

- Le noyau fourni n'est pas pris en charge par GRUB
- Le noyau de rechange n'existe pas

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Utilisez la procédure suivante. <ol style="list-style-type: none">1. Arrêtez l'instance.2. Remplacez-le avec un noyau qui fonctionne.3. Installez un noyau de rechange.4. Modifiez l'AMI en corrigeant le noyau.
Basée sur le stockage d'instance	Utilisez la procédure suivante. <ol style="list-style-type: none">1. Arrêtez l'instance et lancez une nouvelle instance avec le bon noyau.2. Créez une AMI avec le noyau correct.3. (Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

fsck : aucun fichier ou répertoire de ce type lors de la tentative d'ouverture... (système de fichiers non trouvé)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Welcome to Fedora
Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [ OK ]

Starting udev: [ OK ]

Setting hostname localhost: [ OK ]

No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[ OK ]

Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]

*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

Causes potentielles

- Un bogue existe dans les définitions du système de fichiers ramdisk `/etc/fstab`
- Définitions du système de fichiers mal configurées dans `/etc/fstab`
- Lecteur manquant/en échec

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	<p>Utilisez la procédure suivante.</p> <ol style="list-style-type: none">1. Arrêtez l'instance, détachez le volume racine, réparez/modifiez le volume dans le fichier <code>/etc/fstab</code>, attachez le volume à l'instance et lancez l'instance.2. Corrigez le ramdisk pour inclure le fichier <code>/etc/fstab</code> modifié (le cas échéant).3. Modifiez l'AMI pour utiliser un ramdisk plus récent. <p>Le sixième champ de <code>fstab</code> définit les exigences de disponibilité du montage. Une valeur non nulle implique qu'un <code>fsck</code> sera effectué sur ce volume et doit réussir. L'utilisation de ce champ peut être problématique dans Amazon EC2, car un échec entraîne généralement une invite de la console interactive qui n'est actuellement pas disponible dans Amazon EC2. Faites attention avec cette fonction et lisez la page sur la commande <code>man Linux</code> en ce qui concerne <code>fstab</code>.</p>
Basée sur le stockage d'instance	<p>Utilisez la procédure suivante.</p> <ol style="list-style-type: none">1. Mettez fin à l'instance et lancez une nouvelle instance.2. Détachez tous les volumes Amazon EBS errants et l'instance redémarré.3. (Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

General error mounting filesystems (Montage en échec)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting. Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

Causes potentielles

Type d'instance	Cause potentielle
Basée sur Amazon EBS	<ul style="list-style-type: none">• Volume Amazon EBS détaché ou en échec.• Système de fichiers corrompu.• Décalage de la combinaison de ramdisk et d'AMI (par exemple, ramdisk Debian avec une AMI SUSE).
Basée sur le stockage d'instance	<ul style="list-style-type: none">• Un lecteur en échec.• Un système de fichiers corrompu.• Un décalage de la combinaison de ramdisk et d'AMI (par ex., ramdisk Debian avec une AMI SUSE).

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	<p>Utilisez la procédure suivante.</p> <ol style="list-style-type: none">1. Arrêtez l'instance.2. Détachez le volume racine.3. Attachez le volume racine à une instance connue en fonctionnement.4. Exécutez le contrôle du système de fichiers (<code>fsck -a /dev/...</code>).5. Corrigez toutes les erreurs.6. Détachez le volume de l'instance connue en fonctionnement.7. Attachez le volume à l'instance arrêtée.8. Démarrez l'instance.

Pour ce type d'instance	Faire ceci
	9. Revérifiez le statut de l'instance.
Basée sur le stockage d'instance	<p>Essayez l'une des actions suivantes :</p> <ul style="list-style-type: none"> Démarrez une nouvelle instance. (Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

VFS: Unable to mount root fs on unknown-block (le système de fichiers racine ne correspond pas)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line: root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

Causes potentielles

Type d'instance	Cause potentielle
Basée sur Amazon EBS	<ul style="list-style-type: none"> Le périphérique n'est pas attaché correctement. Le périphérique racine n'est pas attaché au bon point périphérique. Le système de fichiers n'est pas au format attendu.

Type d'instance	Cause potentielle
	<ul style="list-style-type: none"> Utilisez le noyau hérité (par exemple, 2.6.16-XenU). Mise à jour récente du noyau sur votre instance (mise à jour défectueuse ou bogue de mise à jour)
Basée sur le stockage d'instance	Échec du périphérique matériel.

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	<p>Effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none"> Arrêtez puis redémarrez l'instance. Modifiez le volume racine pour l'attacher au bon point périphérique, comme <code>/dev/sda1</code> au lieu de <code>/dev/sda</code>. Arrêtez et modifiez pour le noyau moderne. Pour plus d'informations sur les bogues de mise à jour connus, consultez la documentation de votre distribution Linux. Modifiez ou réinstallez le noyau.
Basée sur le stockage d'instance	Arrêtez l'instance et lancez une nouvelle instance en utilisant un noyau moderne.

Erreur : Unable to determine major/minor number of root device... (décalage du système de fichiers/périphérique racine)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

...

```

XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udev[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#

```

Causes potentielles

- Pilote du périphérique de stockage en mode bloc virtuel manquant ou configuré de façon incorrecte
- Conflit de l'énumération du périphérique (sda versus xvda ou sda au lieu de sda1)
- Choix incorrect du noyau de l'instance

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Utilisez la procédure suivante. <ol style="list-style-type: none"> 1. Arrêtez l'instance. 2. Dissociez le volume. 3. Corrigez le problème du mappage du périphérique. 4. Démarrez l'instance. 5. Modifiez l'AMI pour traiter les problèmes du mappage du périphérique.
Basée sur le stockage d'instance	Utilisez la procédure suivante.

Pour ce type d'instance	Faire ceci
	<ol style="list-style-type: none">1. Créez une nouvelle AMI avec la solution appropriée (mapper le périphérique de stockage en mode bloc correctement).2. Arrêtez l'instance et lancez une nouvelle instance à partir de l'AMI que vous avez créée.

XENBUS : Device with no driver...

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udev[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Causes potentielles

- Pilote du périphérique de stockage en mode bloc virtuel manquant ou configuré de façon incorrecte
- Conflit de l'énumération du périphérique (sda versus xvda)
- Choix incorrect du noyau de l'instance

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	<p>Utilisez la procédure suivante.</p> <ol style="list-style-type: none">1. Arrêtez l'instance.2. Dissociez le volume.3. Corrigez le problème du mappage du périphérique.4. Démarrez l'instance.5. Modifiez l'AMI pour traiter les problèmes du mappage du périphérique.
Basée sur le stockage d'instance	<p>Utilisez la procédure suivante.</p> <ol style="list-style-type: none">1. Créez une AMI avec la solution appropriée (mapper le périphérique de stockage en mode bloc correctement).2. Arrêtez l'instance et lancez une nouvelle instance en utilisant l'AMI que vous avez créée.

... days without being checked, check forced (Contrôle du système de fichiers nécessaire)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

Causes potentielles

La durée de contrôle du système de fichiers est dépassée ; un contrôle du système de fichiers est en train d'être forcé.

Actions suggérées

- Patientez jusqu'à ce que le contrôle du système de fichiers se termine. Un contrôle de système de fichiers peut prendre longtemps en fonction de la taille du système de fichiers racine.
- Modifiez vos systèmes de fichiers pour supprimer l'application du contrôle du système de fichiers (fsck) en utilisant tune2fs ou des outils appropriés pour votre système de fichiers.

fsck a échoué à l'état de sortie... (périphérique manquant)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Cleaning up ifupdown....
Loading kernel modules...done.
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
[31mfailed (code 8).[39;49m
```

Causes potentielles

- Ramdisk à la recherche d'un lecteur manquant
- Contrôle de cohérence forcé du système de fichiers
- Lecteur en échec ou détaché

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Essayez une ou plusieurs des solutions suivants pour résoudre le problème :

Pour ce type d'instance	Faire ceci
	<ul style="list-style-type: none">• Arrêtez l'instance, attachez le volume à une instance existante en cours d'exécution.• Exécutez manuellement des contrôles de cohérence.• Corrigez le ramdisk pour inclure les utilitaires pertinents.• Modifiez les paramètres de réglage du système de fichiers pour supprimer les exigences de cohérence (non recommandé).
Basée sur le stockage d'instance	<p>Essayez une ou plusieurs des solutions suivantes pour résoudre le problème :</p> <ul style="list-style-type: none">• Regrouper le ramdisk avec les bons outils.• Modifiez les paramètres de réglage du système de fichiers pour supprimer les exigences de cohérence (non recommandé).• Mettez fin à l'instance et lancez une nouvelle instance.• (Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

Invite GRUB (grubdom>)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
GNU GRUB version 0.97 (629760K lower / 0K upper memory)
```

```
[ Minimal BASH-like line editing is supported. For  
the first word, TAB lists possible command  
completions. Anywhere else TAB lists the possible
```

```
completions of a device/filename. ]
```

```
grubdom>
```

Causes potentielles

Type d'instance	Causes potentielles
Basée sur Amazon EBS	<ul style="list-style-type: none"> Fichier de configuration GRUB manquant. Mauvaise image GRUB utilisée ; fichier de configuration GRUB attendu à un emplacement différent. Système de fichiers non pris en charge utilisé pour stocker votre fichier de configuration GRUB (par exemple, en transformant votre système de fichiers racine en un type qui n'est pas pris en charge par une version plus récente de GRUB).
Basée sur le stockage d'instance	<ul style="list-style-type: none"> Fichier de configuration GRUB manquant. Mauvaise image GRUB utilisée ; fichier de configuration GRUB attendu à un emplacement différent. Système de fichiers non pris en charge utilisé pour stocker votre fichier de configuration GRUB (par exemple, en transformant votre système de fichiers racine en un type qui n'est pas pris en charge par une version plus récente de GRUB).

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Option 1 : Modifiez l'AMI et relancez l'instance :

Pour ce type d'instance	Faire ceci
	<ol style="list-style-type: none">1. Modifiez l'AMI source pour créer un fichier de configuration GRUB à l'emplacement standard (/boot/grub/menu.lst).2. Vérifiez que votre version de GRUB prend en charge le type de système de fichiers sous-jacent et mettez à niveau GRUB si nécessaire.3. Choisissez l'image GRUB appropriée, (hd0 - 1er lecteur ou hd00 – 1er lecteur, première partition).4. Arrêtez l'instance et lancez-en une nouvelle en utilisant l'AMI que vous avez créée. <p>Option 2 : Corrigez l'instance existante:</p> <ol style="list-style-type: none">1. Arrêtez l'instance.2. Détachez le système de fichiers racine.3. Attachez le système de fichiers racine à une instance connue en fonctionnement.4. Montez le système de fichiers.5. Créez un fichier de configuration GRUB.6. Vérifiez que votre version de GRUB prend en charge le type de système de fichiers sous-jacent et mettez à niveau GRUB si nécessaire.7. Détachez le système de fichiers.8. Attachez-le à l'instance originale.9. Modifiez l'attribut noyau pour utiliser l'image GRUB appropriée (1er disque ou 1ère partition sur 1er disque).10. Démarrez l'instance.

Pour ce type d'instance	Faire ceci
Basée sur le stockage d'instance	<p>Option 1 : Modifiez l'AMI et relancez l'instance :</p> <ol style="list-style-type: none">1. Créez la nouvelle AMI avec un fichier de configuration GRUB à l'emplacement standard (/boot/grub/menu.lst).2. Choisissez l'image GRUB appropriée, (hd0 - 1er lecteur ou hd00 – 1er lecteur, première partition).3. Vérifiez que votre version de GRUB prend en charge le type de système de fichiers sous-jacent et mettez à niveau GRUB si nécessaire.4. Arrêtez l'instance et lancez une nouvelle instance en utilisant l'AMI que vous avez créée. <p>Option 2 : Arrêtez l'instance et lancez une nouvelle instance en spécifiant le noyau correct.</p> <div data-bbox="829 1192 1507 1409" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Pour récupérer les données de l'instance existante, contactez AWS Support.</p></div>

Mise en service de l'interface eth0 : l'adresse MAC du périphérique eth0 est différente de celle attendue, ignorer. (Adresse MAC codée de manière irréversible)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

...

```
Bringing up loopback interface: [ OK ]
```

```
Bringing up interface eth0: Device eth0 has different MAC address than expected,  
ignoring.  
[FAILED]
```

```
Starting auditd: [ OK ]
```

Causes potentielles

Il s'agit d'une interface MAC codée en dur dans la configuration d'AMI

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	<p>Effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none">• Modifiez l'AMI pour supprimer le codage en dur et relancez l'instance.• Modifiez l'instance pour supprimer l'adresse MAC codée en dur. <p>OU</p> <p>Utilisez la procédure suivante.</p> <ol style="list-style-type: none">1. Arrêtez l'instance.2. Détachez le volume racine.3. Attachez le volume à une autre instance et modifiez le volume pour supprimer l'adresse MAC codée en dur.4. Attachez le volume à l'instance originale.5. Démarrez l'instance.
Basée sur le stockage d'instance	<p>Effectuez l'une des actions suivantes :</p> <ul style="list-style-type: none">• Modifiez l'instance pour supprimer l'adresse MAC codée en dur.

Pour ce type d'instance	Faire ceci
	<ul style="list-style-type: none">• Mettez fin à l'instance et lancez une nouvelle instance.

Impossible de charger la politique SELinux. L'appareil est en mode d'exécution. Arrêt maintenant. (Erreur de configuration SELinux)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

Causes potentielles

SELinux a été activé par erreur :

- Le noyau fourni n'est pas pris en charge par GRUB
- Le noyau de rechange n'existe pas

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Utilisez la procédure suivante. <ol style="list-style-type: none">1. Arrêtez l'instance en échec.2. Détachez le volume racine de l'instance en échec.3. Attachez le volume racine à une autre instance Linux en fonctionnement (appelée plus tard instance de récupération).

Pour ce type d'instance	Faire ceci
	<ol style="list-style-type: none">Connectez-vous à l'instance de récupération et montez le volume racine de l'instance en échec.Désactivez SELinux sur le volume racine monté. Ce processus varie selon les distributions Linux. Pour plus d'informations, consultez la documentation spécifique à votre système d'exploitation. <div data-bbox="867 632 1507 1136" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Sur certains systèmes, vous désactivez SELinux en réglant <code>SELINUX=disabled</code> dans le fichier <code>/mount_point/etc/sysconfig/selinux</code> où <code>mount_point</code> est l'emplacement où vous avez monté le volume sur votre instance de récupération.</p></div> <ol style="list-style-type: none">Démontez et détachez le volume racine à partir de l'instance de récupération et attachez-le de nouveau à l'instance originale.Démarrez l'instance.
Basée sur le stockage d'instance	Utilisez la procédure suivante. <ol style="list-style-type: none">Mettez fin à l'instance et lancez une nouvelle instance.(Facultatif) Demandez une assistance technique pour la récupération des données en utilisant AWS Support.

XENBUS: Timeout connecting to devices (délai d'attente Xenbus)

Cette condition est indiquée par une entrée du journal du système qui est similaire à celle indiquée ci-dessous.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found. Try passing init= option to kernel.
```

Causes potentielles

- Le périphérique de stockage en mode bloc n'est pas connecté à l'instance
- Cette instance utilise un ancien noyau de l'instance

Actions suggérées

Pour ce type d'instance	Faire ceci
Basée sur Amazon EBS	Effectuez l'une des actions suivantes : <ul style="list-style-type: none">• Modifiez l'AMI et l'instance pour utiliser un noyau moderne et relancez l'instance.• Redémarrez l'instance.
Basée sur le stockage d'instance	Effectuez l'une des actions suivantes : <ul style="list-style-type: none">• Mettez fin à l'instance.• Modifiez l'AMI pour utiliser un noyau moderne et lancez une nouvelle instance en utilisant cette AMI.

Résoudre les problèmes liés au démarrage d'une instance Linux à partir d'un volume incorrect

Note

Cette rubrique de résolution des problèmes s'applique uniquement aux instances Linux.

Dans certaines situations, vous pouvez trouver qu'un volume autre que celui attaché à `/dev/xvda` ou `/dev/sda` est devenu le volume racine de votre instance. Cela peut arriver lorsque vous avez attaché le volume racine d'une autre instance, ou un volume créé à partir de l'instantané d'un volume racine, à une instance avec un volume racine existant.

Ceci est dû à la façon de fonctionner du ramdisk initial dans Linux. Il choisit le volume défini comme `/` dans le fichier `/etc/fstab`, et dans certaines distributions. Ceci est déterminé par l'étiquette attachée à la partition du volume. Plus spécifiquement, vous trouvez que le fichier `/etc/fstab` ressemble à ce qui suit :

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Si vous vérifiez l'étiquette des deux volumes, vous verrez qu'ils contiennent tous les deux l'étiquette `/`:

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

Dans cet exemple, `/dev/xvdf1` pourrait devenir le périphérique racine où votre instance démarre après l'exécution initiale de ramdisk, au lieu du volume `/dev/xvda1` à partir duquel vous aviez essayé de démarrer. Pour résoudre ce problème, utilisez la même commande `e2label` pour changer l'étiquette du volume attaché à partir duquel vous ne souhaitez pas démarrer.

Dans certains cas, spécifier un UUID dans `/etc/fstab` peut résoudre ce problème. Cependant, si les deux volumes proviennent du même instantané ou si le deuxième est créé à partir d'un instantané du volume principal, ils partagent un UUID.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

Pour changer l'étiquette d'un volume ext4 attaché

1. Utilisez la commande `e2label` pour remplacer l'étiquette du volume par autre chose que `/`.

```
[ec2-user ~]$ sudo e2label /dev/xvdf1 old/
```

2. Vérifiez que le volume possède la nouvelle étiquette.

```
[ec2-user ~]$ sudo e2label /dev/xvdf1
old/
```

Pour changer l'étiquette d'un volume xfs attaché

- Utilisez la commande `xfs_admin` pour remplacer l'étiquette du volume par autre chose que `/`.

```
[ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
writing all SBs
new label = "old/"
```

Après avoir modifié l'étiquette du volume comme indiqué, vous devriez pouvoir redémarrer l'instance et avoir le bon volume sélectionné par le ramdisk initial lorsque l'instance démarre.

Important

Si vous prévoyez de détacher le volume avec la nouvelle étiquette et de le renvoyer vers une autre instance pour l'utiliser comme volume racine, vous devez ré-exécuter la procédure ci-

dessus et réattribuer à l'étiquette du volume sa valeur d'origine. Sinon, l'autre instance ne démarre pas, car le ramdisk ne peut pas trouver le volume avec l'étiquette /.

Résoudre les problèmes liés à Sysprep avec les instances Windows

Note

Cette rubrique de résolution des problèmes s'applique uniquement aux instances Windows.

Si vous rencontrez des problèmes ou que vous recevez des messages d'erreur pendant les préparations d'images, consultez les journaux suivants : L'emplacement des journaux varie selon que vous exécutez EC2Config, EC2Launch v1 ou EC2Launch v2 avec Sysprep.

- %WINDIR%\Panther\Unattendgc (EC2Config, EC2Launch v1 et EC2Launch v2)
- %WINDIR%\System32\Sysprep\Panther (EC2Config, EC2Launch v1 et EC2Launch v2)
- C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt (EC2Config uniquement)
- C:\ProgramData\Amazon\Ec2Config\Logs (EC2Config uniquement)
- C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log (EC2Launch v1 uniquement)
- %ProgramData%\Amazon\EC2Launch\log\agent.log (EC2Launch v2 uniquement)

Si vous recevez un message d'erreur pendant la préparation de l'image avec Sysprep, il se peut que le système d'exploitation ne soit pas disponible. Pour consulter les fichiers journaux, vous devez arrêter l'instance, attacher son volume racine à une autre instance saine sur un volume secondaire, puis consulter les journaux mentionnés précédemment sur le volume secondaire. Pour plus d'informations sur l'objectif des fichiers journaux par nom, veuillez consulter [Windows Setup-Related Log Files](#) dans la documentation Microsoft.

Si vous trouvez des erreurs dans le fichier journal Unattendgc, utilisez l'[outil Error Lookup de Microsoft](#) pour en savoir plus sur les erreurs. Le problème suivant signalé dans le fichier journal Unattendgc est généralement dû à un ou plusieurs profils utilisateur corrompus sur l'instance :

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Vous avez deux options à votre disposition pour le résoudre :

Option 1

Utilisez Regedit sur l'instance pour rechercher la clé suivante. Vérifiez qu'il n'existe aucune clé de registre de profil d'utilisateur supprimé.

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
\ProfileList\
```

Option 2

1. Modifiez le fichier concerné, comme suit :

- Windows Server 2012 R2 et version antérieures – Modifiez le fichier de réponses EC2Config (C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml).
- Windows Server 2016 et 2019 – Modifiez le fichier de réponses unattend.xml (C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml).
- Windows Server 2022 – Modifiez le fichier de réponse unattend.xml (C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml).

2. Remplacez `<CopyProfile>true</CopyProfile>` par `<CopyProfile>>false</CopyProfile>`

3. Exécutez à nouveau Sysprep. Notez que cette modification apportée à la configuration entraîne la suppression du profil utilisateur de l'administrateur intégré une fois Sysprep terminé.

Utiliser EC2Rescue pour Linux

EC2Rescue pour Linux est un easy-to-use outil open source qui peut être exécuté sur une instance Amazon EC2 Linux pour diagnostiquer et résoudre les problèmes courants à l'aide de sa bibliothèque de plus de 100 modules. Quelques cas d'utilisation généralisés pour EC2Rescue pour Linux incluent le recueil du journal système et des journaux du gestionnaire de package, la collecte des données d'utilisation des ressources, ainsi que le diagnostic/la résolution des paramètres de noyau problématiques connus et des problèmes OpenSSH courants.

Le runbook [AWS Support - Troubleshoot SSH](#) installe EC2Rescue pour Linux, puis utilise l'outil pour vérifier ou tenter de résoudre les problèmes courants qui empêchent une connexion distante à une machine Linux via SSH. Pour plus d'informations et pour exécuter cette automatisation, consultez [AWS Support-TroubleshootSSH](#).

Si vous utilisez une instance Windows, consultez [the section called "EC2Rescue for Windows Server"](#).

Table des matières

- [Installer EC2Rescue pour Linux](#)
- [Travailler avec EC2Rescue pour Linux](#)
- [Développer des modules EC2Rescue](#)

Installer EC2Rescue pour Linux

L'outil EC2Rescue pour Linux peut être installé sur une instance Amazon EC2 Linux qui satisfait les prérequis suivants.

Prérequis

- Systèmes d'exploitation pris en charge :
 - Amazon Linux 2
 - Amazon Linux 2016.09+
 - SUSE Linux Enterprise Server 12+
 - RHEL 7+
 - Ubuntu 16.04+
- Configuration logicielle requise :
 - Python 2.7.9+ ou 3.2+

Le runbook [AWS Support - Troubleshoot SSH](#) installe EC2Rescue pour Linux, puis utilise l'outil pour vérifier ou tenter de résoudre les problèmes courants qui empêchent une connexion distante à une machine Linux via SSH. Pour plus d'informations et pour exécuter cette automatisation, consultez [AWS Support-TroubleshootSSH](#).

Si votre système dispose de la version Python requise, vous pouvez installer la build standard. Dans le cas contraire, vous pouvez installer la build de la solution groupée, qui inclut une copie minimale de Python.

Pour installer la build standard

1. Sur une instance Linux active, téléchargez l'outil [EC2Rescue pour Linux](#) :

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2r1.tgz
```

2. (Facultatif) Avant de poursuivre, vous pouvez vérifier la signature du fichier d'installation EC2Rescue pour Linux. Pour de plus amples informations, veuillez consulter [\(Facultatif\) Vérification de la signature de EC2Rescue pour Linux](#).

3. Téléchargez le fichier de hachage sha256 :

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2r1.tgz.sha256
```

4. Vérifiez l'intégrité du tarball :

```
sha256sum -c ec2r1.tgz.sha256
```

5. Déballez le tarball :

```
tar -xzvf ec2r1.tgz
```

6. Vérifiez l'installation en énumérant le fichier d'aide :

```
cd ec2r1-<version_number>  
./ec2r1 help
```

Pour installer la build de la solution groupée

Pour obtenir un lien jusqu'à la page de téléchargement et la liste des restrictions, consultez [EC2Rescue pour Linux](#) sur github.

(Facultatif) Vérification de la signature de EC2Rescue pour Linux

La procédure suivante est celle recommandée pour vérifier la validité du package EC2Rescue pour Linux pour les systèmes d'exploitation Linux.

Lorsque vous téléchargez une application à partir d'Internet, nous vous recommandons d'authentifier l'identité de l'éditeur du logiciel et de vérifier que l'application n'a pas été modifiée ou corrompue depuis sa publication. Cela vous évitera d'installer une version de l'application contenant un virus ou tout autre code malveillant.

Si, après l'exécution de la procédure décrite dans cette rubrique, vous déterminez que le logiciel de EC2Rescue pour Linux a été modifié ou corrompu, n'exécutez pas le fichier d'installation. Contactez plutôt Amazon Web Services.

Les fichiers EC2Rescue pour Linux pour les systèmes d'exploitation Linux sont signés à l'aide de GnuPG, une mise en œuvre Open Source de la norme Pretty Good Privacy (OpenPGP) pour les signatures numériques sécurisées. GnuPG (également connu sous le nom de GPG) fournit une authentification et un contrôle d'intégrité par le biais d'une signature numérique. AWS publie une clé publique et des signatures que vous pouvez utiliser pour vérifier le package EC2Rescue pour Linux téléchargé. Pour plus d'informations sur PGP et GnuPG (GPG), consultez <http://www.gnupg.org>.

La première étape consiste à établir une approbation avec l'éditeur du logiciel. Téléchargez la clé publique de l'éditeur du logiciel, vérifiez que le propriétaire de cette clé publique est bien celui qu'il prétend être, puis ajoutez la clé publique à votre porte-clés. Votre porte-clés est un ensemble de clés publiques connues. Après avoir établi l'authenticité de la clé publique, vous pouvez l'utiliser pour vérifier la signature de l'application.

Tâches

- [Installation des outils GPG](#)
- [Authentification et importation de la clé publique](#)
- [Vérification de la signature du package](#)

Installation des outils GPG

Si votre système d'exploitation est Linux ou Unix, les outils GPG peuvent déjà être installés. Pour tester si les outils sont installés sur votre système, entrez `gpg2` à partir d'une invite de commande. Si les outils GPG sont installés, une invite de commande GPG s'affiche. Si les outils GPG ne sont pas installés, vous voyez une erreur indiquant que la commande est introuvable. Vous pouvez installer le package GnuPG à partir d'un référentiel.

Pour installer les outils GPG sur un système Linux basé sur Debian

- Depuis un terminal, exécutez la commande suivante :

```
apt-get install gnupg2
```

Pour installer les outils GPG sur un système Linux basé sur Red Hat

- Depuis un terminal, exécutez la commande suivante :

```
yum install gnupg2
```

Authentification et importation de la clé publique

L'étape suivante consiste à authentifier la clé publique EC2Rescue pour Linux et à l'ajouter en tant que clé de confiance à votre porte-clés GPG.

Pour authentifier et importer la clé publique EC2Rescue pour Linux

1. À l'invite de commande, utilisez la commande suivante pour obtenir une copie de votre clé publique GPG :

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2r1.key
```

2. À l'invite de commande, dans le répertoire où vous avez enregistré `ec2r1.key`, exécutez la commande suivante pour importer la clé publique EC2Rescue pour Linux dans votre porte-clés :

```
gpg2 --import ec2r1.key
```

La commande renvoie un résultat semblable à ce qui suit :

```
gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

Vérification de la signature du package

Après avoir installé les outils GPG, authentifié et importé la clé publique d'EC2Rescue pour Linux et vérifié que la clé publique d'EC2Rescue pour Linux est approuvée, vous êtes prêt à vérifier la signature du script d'installation d'EC2Rescue pour Linux.

Pour vérifier la signature du script d'installation EC2Rescue pour Linux

1. À l'invite de commande, exécutez la commande suivante pour télécharger le fichier signature du script d'installation :

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2r1.tgz.sig
```

2. Vérifiez la signature en exécutant la commande suivante à l'invite de commande dans le répertoire où vous avez enregistré `ec2r1.tgz.sig` et le fichier d'installation d'EC2Rescue pour Linux. Ces deux fichiers doivent être présents.

```
gpg2 --verify ./ec2r1.tgz.sig
```

Le résultat doit ressembler à ce qui suit :

```
gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
```

Si le résultat contient l'expression `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`, cela signifie que la signature a été vérifiée et vous pouvez continuer à exécuter le script d'installation d'EC2Rescue pour Linux.

Si le résultat inclut l'expression `BAD signature`, vérifiez si vous avez effectué la procédure correctement. Si vous continuez à obtenir cette réponse, contactez Amazon Web Services et n'exécutez pas le fichier d'installation que vous avez précédemment téléchargé.

Voici les informations détaillées sur les avertissements qui peuvent s'afficher :

- **WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner.** Ce message fait référence à votre niveau de confiance personnel dans la conviction que vous possédez une clé publique authentique pour EC2Rescue pour Linux. Dans un monde idéal, vous visiteriez un bureau Amazon Web Services et recevriez la clé en personne. Cependant, vous la téléchargez le plus souvent à partir d'un site Web. Dans le cas présent, le site Web est un site Amazon Web Services.

- gpg2: no ultimately trusted keys found. Cela signifie que la clé spécifique n'est pas « approuvée en dernier lieu » par vous-même (ou par d'autres personnes de confiance).

Pour plus d'informations, consultez <http://www.gnupg.org>.

Travailler avec EC2Rescue pour Linux

Les tâches suivantes sont des tâches courantes que vous pouvez effectuer pour commencer à utiliser cet outil.

Tâches

- [Exécutez EC2Rescue pour Linux](#)
- [Charger les résultats](#)
- [Créer des sauvegardes](#)
- [Obtenir de l'aide](#)

Exécutez EC2Rescue pour Linux

Vous pouvez exécuter EC2Rescue pour Linux, comme illustré dans les exemples suivants..

Exemple Exemple : Exécuter tous les modules

Pour exécuter tous les modules, exécutez EC2Rescue pour Linux sans options :

```
./ec2r1 run
```

Certains modules nécessitent un accès racine. Si vous n'êtes pas un utilisateur racine, utilisez sudo pour exécuter ces modules comme suit :

```
sudo ./ec2r1 run
```

Exemple Exemple : Exécuter un module spécifique

Pour exécuter uniquement des modules spécifiques, utilisez le paramètre --only-modules :

```
./ec2r1 run --only-modules=module_name --arguments
```

Par exemple, cette commande exécute le module dig pour interroger le domaine amazon.com :

```
./ec2r1 run --only-modules=dig --domain=amazon.com
```

Exemple Exemple : Afficher les résultats

Vous pouvez afficher les résultats dans `/var/tmp/ec2r1`:

```
cat /var/tmp/ec2r1/logfile_location
```

Par exemple, affichez le fichier journal pour le module dig :

```
cat /var/tmp/ec2r1/2017-05-11T15_39_21.893145/mod_out/run/dig.log
```

Charger les résultats

Si vous avez AWS Support demandé les résultats ou si vous souhaitez partager les résultats depuis un compartiment S3, téléchargez-les à l'aide de l'outil CLI EC2Rescue pour Linux. La sortie des commandes EC2Rescue pour Linux doit fournir les commandes que vous avez besoin d'utiliser.

Exemple Exemple : télécharger les résultats vers AWS Support

```
./ec2r1 upload --upload-directory=/var/tmp/ec2r1/2017-05-11T15_39_21.893145 --support-url="URLProvidedByAWSsupport"
```

Exemple Exemple : Charger les résultats dans un compartiment S3

```
./ec2r1 upload --upload-directory=/var/tmp/ec2r1/2017-05-11T15_39_21.893145 --presigned-url="YourPresignedS3URL"
```

Pour plus d'informations sur la génération d'URL pré-signées pour Amazon S3, consultez [Téléchargement d'objets utilisant des URL pré-signées](#).

Créer des sauvegardes

Créez une sauvegarde pour votre instance, un ou plusieurs volumes, ou un ID d'appareil spécifique à l'aide des commandes suivantes.

Exemple Exemple : Sauvegarder une instance avec une Amazon Machine Image (AMI)

```
./ec2r1 run --backup=ami
```

Exemple Exemple : Sauvegarder tous les volumes associés à l'instance

```
./ec2r1 run --backup=allvolumes
```

Exemple Exemple : Sauvegarder un volume spécifique

```
./ec2r1 run --backup=volumeID
```

Obtenir de l'aide

EC2Rescue pour Linux inclut un fichier d'aide qui vous fournit des informations et la syntaxe pour chaque commande disponible.

Exemple Exemple : Afficher l'aide générale

```
./ec2r1 help
```

Exemple Exemple : Répertorier les modules disponibles

```
./ec2r1 list
```

Exemple Exemple : Afficher l'aide pour un module spécifique

```
./ec2r1 help module_name
```

Par exemple, utilisez la commande suivante pour afficher le fichier d'aide pour le module dig :

```
./ec2r1 help dig
```

Développer des modules EC2Rescue

Les modules sont écrits en YAML, une norme de sérialisation des données. Le fichier YAML d'un module se compose d'un document unique, qui représente le module et ses attributs.

Ajouter des attributs de module

Le tableau suivant répertorie les attributs de module disponibles.

Attribut	Description
name	Nom du module. La longueur du nom doit être inférieure ou égale à 18 caractères.
Version	Numéro de version du module.
title	Titre court et descriptif du module. La longueur de cette valeur doit être inférieure ou égale à 50 caractères.
helptext	<p>Description étendue du module. La longueur de chaque ligne doit être inférieure ou égale à 75 caractères. Si le module consomme des arguments, obligatoires ou facultatifs, incluez-les dans la valeur helptext.</p> <p>Exemples :</p> <pre>helptext: !!str Collect output from ps for system analysis Consumes --times= for number of times to repeat Consumes --period= for time period between repetition</pre>
placement	<p>Étape dans laquelle le module doit être exécuté. Valeurs prises en charge :</p> <ul style="list-style-type: none">• prediagnostic• run• postdiagnostic
langage	<p>Langage dans lequel le code du module est écrit. Valeurs prises en charge :</p> <ul style="list-style-type: none">• bash• python

Attribut	Description
	<p> Note</p> <p>Le code Python doit être compatible avec Python 2.7.9+ et Python 3.2+.</p>
remediation	<p>Indique si le module prend en charge la correction. Les valeurs prises en charge sont <code>True</code> ou <code>False</code>.</p> <p>Le module utilise par défaut <code>False</code> si aucune valeur n'est indiquée. Il s'agit donc d'un attribut facultatif pour les modules qui ne prennent pas en charge la correction.</p>
content	Intégralité du code de script.
contrainte	Nom de l'objet contenant les valeurs de contrainte.
domaine	<p>Descripteur de la façon dont le module est regroupé ou classé. L'ensemble de modules inclus utilise les domaines suivants :</p> <ul style="list-style-type: none">• application• net• os• performances

Attribut	Description
class	<p>Descripteur du type de tâche effectué par le module. L'ensemble de modules inclus utilise les classes suivantes :</p> <ul style="list-style-type: none">• collect (collecte la sortie des programmes)• diagnose (réussite/échec en fonction d'un ensemble de critères)• gather (copie les fichiers et écrit dans un fichier spécifique)
distro	<p>Liste des distributions Linux que ce module prend en charge. L'ensemble de modules inclus utilise les distributions suivantes :</p> <ul style="list-style-type: none">• alami (Amazon Linux)• rhel• ubuntu• suse
obligatoire	<p>Arguments obligatoires que le module consomme à partir des options de la CLI.</p>
facultatif	<p>Arguments facultatifs que le module peut utiliser.</p>
logiciel	<p>Exécutables logiciels utilisés dans le module. Cet attribut a pour but de spécifier un logiciel qui n'est pas installé par défaut. La logique EC2Rescue pour Linux s'assure que ces programmes sont présents et exécutables avant l'exécution du module.</p>

Attribut	Description
package	Package logiciel source pour un exécutable. Cet attribut a pour but de fournir des détails étendus sur le package avec le logiciel, y compris une URL pour le téléchargement ou pour obtenir de plus amples informations.
sudo	<p>Indique si l'accès racine est obligatoire pour exécuter le module.</p> <p>Vous n'avez pas besoin d'implémenter des vérifications sudo dans le script du module. Si la valeur est true, la logique EC2Rescue pour Linux exécute uniquement le module lorsque l'utilisateur qui exécute le module possède un accès racine.</p>
perfimpact	Indique si le module peut avoir un impact important sur les performances qui affecte l'environnement dans lequel il est exécuté. Si la valeur est true et que l'argument <code>--perfimpact=true</code> n'est pas présent, le module est ignoré.
parallexclusive	Spécifie un programme qui requiert une exclusivité mutuelle. Par exemple, tous les modules qui spécifient « bpf » sont exécutés en série.

Ajouter des variables d'environnement

Le tableau suivant répertorie les variables d'environnement disponibles.

Variable d'environnement	Description
EC2RL_CALLPATH	Chemin vers <code>ec2rl.py</code> . Ce chemin peut être utilisé pour localiser le répertoire <code>lib</code> et utiliser les modules Python fournis.
EC2RL_WORKDIR	Répertoire <code>tmp</code> principal pour l'outil de diagnostic. Valeur par défaut: <code>/var/tmp/ec2rl</code> .
EC2RL_RUNDIR	Répertoire dans lequel toutes les sorties sont stockées. Valeur par défaut: <code>/var/tmp/ec2rl/<date&timestamp></code> .
EC2RL_GATHEREDDIR	Répertoire racine dans lequel placer les données collectées sur le module. Valeur par défaut: <code>/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/</code> .
EC2RL_NET_DRIVER	Pilote utilisé pour la première interface réseau non virtuelle, triée par ordre alphabétique, de l'instance. Exemples : <ul style="list-style-type: none">• <code>xen_netfront</code>• <code>ixgbevf</code>• <code>ena</code>
EC2RL_SUDO	True si EC2Rescue pour Linux est en cours d'exécution en tant que racine ; sinon la valeur est false.

Variable d'environnement	Description
EC2RL_VIRT_TYPE	Type de virtualisation, tel que fourni par les métadonnées d'instance. Exemples : <ul style="list-style-type: none">• default-hvm• default-paravirtual
EC2RL_INTERFACES	Liste énumérée des interfaces du système. La valeur est une chaîne contenant des noms, tels que <code>eth0</code> , <code>eth1</code> , etc. Elle est générée via <code>functions.bash</code> et est disponible uniquement pour les modules dont elle provient.

Utiliser la syntaxe YAML

Tenez compte des points suivants lorsque vous créez vos fichiers YAML de module :

- Le triple trait d'union (`---`) indique le début explicite d'un document.
- La balise `!ec2rlcore.module.Module` indique à l'analyseur YAML le constructeur à appeler lors de la création de l'objet à partir du flux de données. Vous trouverez le constructeur dans le fichier `module.py`.
- La balise `!!str` indique à l'analyseur YAML de ne pas tenter de déterminer le type des données, et d'interpréter plutôt le contenu comme un littéral de chaîne.
- Le caractère pipe (`|`) indique à l'analyseur YAML que la valeur est une scalaire littérale. Dans ce cas, l'analyseur inclut tous les espaces. C'est important pour les modules car les caractères de mise en retrait et de saut de ligne sont conservés.
- La mise en retrait standard YAML correspond à deux espaces, comme illustré dans les deux exemples suivants. Veillez à conserver la mise en retrait standard (par exemple, quatre espaces pour Python) pour votre script, puis mettez en retrait l'intégralité du contenu à l'aide de deux espaces dans le fichier du module.

Exemples de modules

Exemple un (mod.d/ps.yaml):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
    printf "%0.s=" {1..80}
    echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
    exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
  $period seconds."
  for i in $(seq 1 $times); do
    ps auxww
    sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
```

```
sudo: !!str False
perfimpact: !!str False
parallexclusive: !!str
```

Utiliser EC2Rescue for Windows Server

EC2Rescue for Windows Server est un easy-to-use outil que vous exécutez sur une instance Amazon EC2 Windows Server pour diagnostiquer et résoudre d'éventuels problèmes. Il est utile non seulement pour collecter les fichiers journaux et résoudre les problèmes, mais aussi pour rechercher de manière proactive les éventuels sujets de préoccupation. Il permet même d'examiner les volumes racine Amazon EBS pour d'autres instances et de collecter les journaux correspondants à des fins de dépannage des instances Windows Server à l'aide de ce volume.

EC2Rescue for Windows Server est composé de deux modules distincts : un module de collecte de données qui permet de collecter les données auprès de l'ensemble des différentes sources et un module d'analyse qui permet de comparer les données collectées à une série de règles prédéfinies afin d'identifier les problèmes et d'offrir des suggestions.

L'outil EC2Rescue pour Windows Server s'exécute uniquement sur les instances Amazon EC2 exécutant Windows Server 2012 et versions ultérieures. Lorsque l'outil démarre, il vérifie s'il s'exécute sur une instance Amazon EC2.

Le runbook `AWSSupport-ExecuteEC2Rescue` utilise l'outil EC2Rescue pour dépanner et réparer, si possible, les problèmes de connectivité courants avec l'instance EC2 spécifiée. Pour plus d'informations et pour exécuter cette automatisation, consultez [AWSSupport-ExecuteEC2Rescue](#).

Si vous utilisez une instance Linux, consultez [the section called "EC2Rescue for Linux"](#).

Table des matières

- [Utiliser l'interface graphique EC2Rescue for Windows Server](#)
- [Utiliser EC2Rescue for Windows Server avec la ligne de commande](#)
- [Utiliser EC2Rescue for Windows Server avec Run Command Systems Manager](#)

Utiliser l'interface graphique EC2Rescue for Windows Server

EC2Rescue for Windows Server peut effectuer l'analyse suivante sur les instance hors ligne :

Option	Description
Diagnostic et résolution des problèmes	<p>EC2Rescue for Windows Server peut détecter et résoudre des problèmes avec les paramètres de service suivants :</p> <ul style="list-style-type: none">• Heure du système<ul style="list-style-type: none">• RealTimeisUniversal - Détecte si la clé de RealTimeisUniversal registre est activée. Si ce paramètre est désactivé , l'heure du système Windows s'écarte lorsque le fuseau horaire est définie sur une autre valeur qu'UTC.• Pare-feu Windows<ul style="list-style-type: none">• Réseaux de domaine : détectent si ce profil de pare-feu Windows est activé ou désactivé.• Réseaux privés : détectent si ce profil de pare-feu Windows est activé ou désactivé.• Réseaux invités ou publics : détectent si ce profil de pare-feu Windows est activé ou désactivé.• Bureau à distance<ul style="list-style-type: none">• Démarrage du service : détecte si le service bureau à distance est activé.• Connexions réseau à distance : détectent si cette option est activée.• Port TCP : détecte le port sur lequel le service Bureau à distance écoute.• EC2Config (Windows Server 2012 R2 et antérieures)

Option	Description
	<ul style="list-style-type: none">• Installation : détecte la version EC2Config qui est installée.• Démarrage du service : détecte si le service EC2Config est activé.• Ec2 SetPassword - Génère un nouveau mot de passe administrateur.• Ec2 HandleUser Data - Vous permet d'exécuter un script de données utilisateur lors du prochain démarrage de l'instance. <ul style="list-style-type: none">• EC2Launch (Windows Server 2016 et versions ultérieures)<ul style="list-style-type: none">• Installation : détecte la version EC2Launch qui est installée.• Ec2 SetPassword - Génère un nouveau mot de passe administrateur. <ul style="list-style-type: none">• Interface réseau<ul style="list-style-type: none">• Démarrage du service DHCP : détecte si le service DHCP est activé.• Détails Ethernet : affiche des informations détaillées sur la version de pilote réseau, si elle est détectée.• DHCP sur Ethernet : détecte si le service DHCP est activé. <ul style="list-style-type: none">• État de signature de disque<ul style="list-style-type: none">• Signature on disk (Signature de disque) et Signature on Boot Configuration Database (BCD) (Signature BCD) : détecte si la signature de disque et la signature BCD sont identiques. Si les valeurs sont

Option	Description
	différentes, EC2Rescue tente d'écraser la signature de disque par la signature BCD.
Restaurer	<p>Effectuez l'une des opérations suivantes :</p> <ul style="list-style-type: none"> • Dernière configuration correcte connue : tente de démarrer l'instance avec son dernier état de démarrage connu. • Restaurer le registre à partir de la sauvegarde : restaure le registre à partir de <code>\Windows\System32\config\RegBack</code> .
Capture Logs	Permet de capturer des journaux sur l'instance en vue de les analyser.

EC2Rescue for Windows Server peut collecter les données suivantes à partir des instances actives et hors ligne :

Élément	Description
Event Log	Collecte les journaux d'événements d'application, de système et EC2Config.
Registre	Collecte les ruches SYSTEM et SOFTWARE.
Windows Update Log	<p>Permet de collecter les fichiers journaux générés par Windows Update.</p> <div data-bbox="829 1507 1508 1822" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Dans Windows Server 2016 et les versions ultérieures, le journal est collecté au format Event Tracing for Windows (ETW).</p> </div>

Élément	Description
Sysprep Log	Permet de collecter les fichiers journaux générés par l'outil Windows System Preparation.
Journal de configuration du pilote	Collecte les journaux Windows SetupAPI (setupapi.dev.log et setupapi.setup.log).
Boot Configuration	Collecte la ruche HKEY_LOCAL_MACHINE\BCD00000000.
Memory Dump	Permet de collecter les fichiers de vidage de mémoire existant sur l'instance.
Fichier EC2Config	Permet de collecter les fichiers journaux générés par le service EC2Config.
EC2Launch File	Permet de collecter les fichiers journaux générés par les scripts EC2Launch.
SSM Agent File	Permet de collecter les fichiers journaux générés par SSM Agent et les journaux Patch Manager.
Fichier GPU Elastic EC2	Collecte les journaux d'événements liés à des GPU Elastic.
ECS	Permet de collecter les journaux liés à Amazon ECS.
CloudEndure	Collecte les fichiers journaux relatifs à CloudEndure l'agent.

EC2Rescue for Windows Server peut collecter les données supplémentaires suivantes à partir des instances actives :

Élément	Description
System Information	Permet de collecter MSInfo32.
Résultat de la politique de groupe	Collecte un rapport de politique de groupe.

Analyser une instance hors connexion

L'option Offline Instance (Instance hors ligne) est pratique pour déboguer les problèmes de démarrage liés aux instances Windows.

Pour effectuer une action sur une instance hors ligne

1. Sur une instance Windows Server active, téléchargez l'outil [EC2Rescue for Windows Server](#) et extrayez les fichiers.

Vous pouvez exécuter la PowerShell commande suivante pour télécharger EC2Rescue sans modifier votre configuration de sécurité renforcée (ESC) d'Internet Explorer :

```
Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -  
OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Cette commande télécharge le fichier EC2Rescue .zip sur le bureau de l'utilisateur actuellement connecté.

Note

Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, le protocole TLS 1.2 devra peut-être être activé sur votre PowerShell terminal. Vous pouvez activer le protocole TLS 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol =  
[Net.SecurityProtocolType]::Tls12
```

2. Arrêtez l'instance défaillante si ce n'est pas déjà fait.

3. Détachez le volume racine EBS d'une instance défectueuse et attachez-le à une instance Windows active sur laquelle EC2Rescue for Windows Server est installé.
4. Exécutez l'outil EC2Rescue for Windows Server sur l'instance active et choisissez Offline Instance (Instance hors ligne).
5. Sélectionnez le disque du volume nouvellement monté et choisissez Next (Suivant).
6. Confirmez la sélection de disque et choisissez Yes (Oui).
7. Choisissez l'option d'instance en ligne à exécuter puis sélectionnez Next (Suivant).

L'outil EC2Rescue for Windows Server analyse le volume et collecte des informations de dépannage basées sur les fichiers journaux sélectionnés.

Collecter des données à partir d'une instance active

Vous pouvez collecter des journaux et d'autres données à partir d'une instance active

Pour collecter des données à partir d'une instance active

1. Connectez-vous à votre instance Windows.
2. Téléchargez l'outil [EC2Rescue for Windows Server](#) sur votre instance Windows et extrayez les fichiers..

Vous pouvez exécuter la PowerShell commande suivante pour télécharger EC2Rescue sans modifier votre configuration de sécurité renforcée (ESC) d'Internet Explorer :

```
Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -  
OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Cette commande télécharge le fichier EC2Rescue .zip sur le bureau de l'utilisateur actuellement connecté.

Note

Si un message d'erreur s'affiche lors du téléchargement du fichier et que vous utilisez Windows Server 2016 ou une version antérieure, le protocole TLS 1.2 devra peut-être être activé sur votre PowerShell terminal. Vous pouvez activer le protocole TLS 1.2 pour la PowerShell session en cours à l'aide de la commande suivante, puis réessayer :

```
[Net.ServicePointManager]::SecurityProtocol =  
[Net.SecurityProtocolType]::Tls12
```

3. Ouvrez l'application EC2Rescue for Windows Server et acceptez le contrat de licence.
4. Choisissez Next (Suivant), Current instance (Instance actuelle), Capture logs (Capturer les journaux).
5. Sélectionnez les éléments de données à collecter et choisissez Collect... (Collecter...). Lisez l'avertissement et choisissez Yes (Oui) pour continuer.
6. Choisissez un nom de fichier et un emplacement pour le fichier ZIP et cliquez sur Save (Enregistrer).
7. Lorsqu'EC2Rescue for Windows Server a terminé, choisissez Open Containing Folder (Ouvrir le dossier contenant) pour afficher le fichier ZIP.
8. Choisissez Finish.

Utiliser EC2Rescue for Windows Server avec la ligne de commande

L'interface de ligne de commande (CLI) EC2Rescue for Windows Server vous permet d'exécuter un plug-in EC2Rescue for Windows Server (appelé « action ») par programmation.

L'outil EC2Rescue for Windows Server a deux modes d'exécution :

- `/online` (/en ligne) — Cela vous permet d'exécuter une action sur l'instance sur laquelle EC2Rescue for Windows Server est installé, par exemple, collecter des fichiers journaux.
- `/offline: (/hors ligne :)<device_id>` — Cela vous permet d'exécuter une action sur le volume racine hors connexion qui est attaché à une instance Amazon EC2 Windows distincte, où vous avez installé EC2Rescue for Windows Server.

Téléchargez l'outil [EC2Rescue for Windows Server](#) sur votre instance Windows et extrayez les fichiers.. Vous pouvez afficher le fichier d'aide avec la commande suivante :

```
EC2RescueCmd.exe /help
```

EC2Rescue for Windows Server peut effectuer les actions suivantes sur une instance Amazon EC2 Windows :

- [Action de collecte](#)
- [Action de résolution](#)
- [Action de restauration](#)

Action de collecte

Note

Vous pouvez collecter tous les journaux, un groupe de journaux complet ou un journal individuel au sein d'un groupe.

EC2Rescue for Windows Server peut collecter les données suivantes à partir des instances actives et hors ligne.

Groupe de journaux	Journaux disponibles	Description
all		Collecte tous les journaux disponibles.
eventlog	<ul style="list-style-type: none">• 'Application'• 'System'• 'EC2ConfigService'	Collecte les journaux d'événements d'application, de système et EC2Config.
memory-dump	<ul style="list-style-type: none">• 'Memory Dump File'• 'Mini Dump Files'	Permet de collecter les fichiers de vidage de mémoire existant sur l'instance.
ec2config	<ul style="list-style-type: none">• 'Log Files'• 'Configuration Files'	Permet de collecter les fichiers journaux générés par le service EC2Config.
ec2launch	<ul style="list-style-type: none">• 'Logs'• 'Config'	Permet de collecter les fichiers journaux générés par les scripts EC2Launch.

Groupe de journaux	Journaux disponibles	Description
ssm-agent	<ul style="list-style-type: none">'Log Files''Patch Baseline Logs''InstanceData'	Permet de collecter les fichiers journaux générés par SSM Agent et les journaux Patch Manager.
sysprep	'Log Files'	Permet de collecter les fichiers journaux générés par l'outil Windows System Preparation.
driver-setup	<ul style="list-style-type: none">'SetupAPI Log Files''DPIInst Log File''AWS PV Setup Log File'	Collecte les journaux Windows SetupAPI (setupapi.dev.log et setupapi.setup.log).
registry	<ul style="list-style-type: none">'SYSTEM''SOFTWARE''BCD'	Collecte les ruches SYSTEM et SOFTWARE.
egpu	<ul style="list-style-type: none">'Event Log''System Files'	Collecte les journaux d'événements liés à des GPU Elastic.
boot-config	'BCDEDIT Output'	Collecte la ruche HKEY_LOCAL_MACHINE\BCD00000000 .

Groupe de journaux	Journaux disponibles	Description
windows-update	'Log Files'	Permet de collecter les fichiers journaux générés par Windows Update. <div data-bbox="1068 401 1511 856" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>Dans Windows Server 2016 et les versions ultérieures, le journal est collecté au format Event Tracing for Windows (ETW).</p> </div>
cloudendure	<ul style="list-style-type: none"> • 'Migrate Script Logs' • 'Driver Logs' • 'CloudEndure File List' 	Collecte les fichiers journaux relatifs à CloudEndure l'agent.

EC2Rescue for Windows Server peut collecter les données supplémentaires suivantes à partir des instances actives.

Groupe de journaux	Journaux disponibles	Description
system-info	'MSInfo32 Output'	Collecte MSInfo32.
gpresult	'GPResult Output'	Collecte un rapport de politique de groupe.

Les options suivantes sont disponibles :

- /output : <output FilePath > - Emplacement du chemin du fichier de destination requis pour enregistrer les fichiers journaux collectés au format zip.

- `/no-offline` : attribut facultatif utilisé en mode hors ligne. Ne met pas le volume hors connexion après avoir exécuté l'action.
- `/no-fix-signature` : attribut facultatif utilisé en mode hors ligne. Ne corrige pas une collision de signature de disque possible après avoir exécuté l'action.

Exemples

Voici des exemples d'utilisation de la CLI EC2Rescue for Windows Server.

Exemples en mode en ligne

Collecter tous les journaux disponibles :

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Collecter uniquement un groupe de journaux spécifique :

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Collecter des journaux individuels au sein d'un groupe de journaux :

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI  
Log Files' /output:<outputFilePath>
```

Exemples de mode hors connexion

Collecter tous les journaux disponibles à partir d'un volume EBS. Le volume est spécifié par la valeur d'ID de périphérique.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Collecter uniquement un groupe de journaux spécifique :

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Action de résolution

EC2Rescue for Windows Server peut détecter et résoudre des problèmes avec les paramètres de service suivants :

Groupe de services	Actions disponibles	Description
all		
system-time	'RealTimeIsUniversal'	<p>Heure du système</p> <ul style="list-style-type: none"> RealTimeIsUniversal - Détecte si la clé de RealTimeIsUniversal registre est activée. Si ce paramètre est désactivé, l'heure du système Windows s'écarte lorsque le fuseau horaire est définie sur une autre valeur qu'UTC.
firewall	<ul style="list-style-type: none"> 'Domain networks' 'Private networks' 'Guest or public networks' 	<p>Pare-feu Windows</p> <ul style="list-style-type: none"> Réseaux de domaine : détectent si ce profil de pare-feu Windows est activé ou désactivé. Réseaux privés : détectent si ce profil de pare-feu Windows est activé ou désactivé. Réseaux invités ou publics : détectent si ce profil de pare-feu Windows est activé ou désactivé.
rdp	<ul style="list-style-type: none"> 'Service Start' 'Remote Desktop Connections' 'TCP Port' 	<p>Bureau à distance</p> <ul style="list-style-type: none"> Démarrage du service : détecte si le service bureau à distance est activé.

Groupe de services	Actions disponibles	Description
		<ul style="list-style-type: none"> • Connexions réseau à distance : détectent si cette option est activée. • Port TCP : détecte le port sur lequel le service Bureau à distance écoute.
ec2config	<ul style="list-style-type: none"> • 'Service Start' • 'Ec2SetPassword' • 'Ec2HandleUserData' 	<p>EC2Config</p> <ul style="list-style-type: none"> • Démarrage du service : détecte si le service EC2Config est activé. • Ec2 SetPassword - Génère un nouveau mot de passe administrateur. • Ec2 HandleUser Data - Vous permet d'exécuter un script de données utilisateur lors du prochain démarrage de l'instance.
ec2launch	'Reset Administrator Password'	Génère un nouveau mot de passe administrateur Windows.
network	'DHCP Service Startup'	<p>Interface réseau</p> <ul style="list-style-type: none"> • Démarrage du service DHCP : détecte si le service DHCP est activé.

Les options suivantes sont disponibles :

- `/level:<level>` : attribut facultatif pour le niveau de contrôle que l'action doit déclencher. Les valeurs autorisées sont les suivantes: `information`, `warning`, `error`, `all`. Par défaut, l'attribut est défini sur `error`.
- `/check-only` : attribut facultatif qui génère un rapport mais n'effectue aucune modification sur le volume hors ligne.

Note

Si EC2Rescue pour Windows Server détecte une possible collision de signature de disque, il corrige la signature une fois le processus hors ligne terminé par défaut, même lorsque vous utilisez `/check-only` option. Vous devez utiliser `/no-fix-signature` cette option pour empêcher la correction.

- `/no-offline` : attribut facultatif qui empêche la mise hors ligne du volume une fois l'action exécutée.
- `/no-fix-signature` : attribut facultatif qui ne corrige pas une collision de signature de disque possible après avoir exécuté l'action.

Exemples de résolution

Voici des exemples d'utilisation de la CLI EC2Rescue for Windows Server. Le volume est spécifié à l'aide de la valeur d'ID de périphérique.

Tenter de corriger tous les problèmes identifiés sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Tenter de corriger tous les problèmes identifiés au sein d'un groupe de services sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Tenter de corriger un élément spécifique au sein d'un groupe de services sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Spécifier plusieurs problèmes à tenter de corriger sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-time.RealTimeIsUniversal,ec2config.Service Start'
```

Action de restauration

EC2Rescue for Windows Server peut détecter et résoudre des problèmes avec les paramètres de service suivants :

Groupe de services	Actions disponibles	Description
Restaurer la dernière configuration correcte connue	lkgc	Dernière configuration correcte connue : tente de démarrer l'instance avec son dernier état de démarrage connu.
Restaurer le registre Windows à partir de la dernière sauvegarde	regback	Restaurer le registre à partir de la sauvegarde : restaure le registre à partir de \Windows\System32\config\RegBack .

Les options suivantes sont disponibles :

- /no-offline — Attribut facultatif qui empêche la mise hors connexion du volume une fois l'action exécutée.
- /no-fix-signature — Attribut facultatif qui ne corrige pas une collision de signature de disque possible après avoir exécuté l'action.

Exemples de restauration

Voici des exemples d'utilisation de la CLI EC2Rescue for Windows Server. Le volume est spécifié à l'aide de la valeur d'ID de périphérique.

Restaurer la dernière configuration correcte connue sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Restaurer la dernière sauvegarde du registre Windows sur un volume :

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Utiliser EC2Rescue for Windows Server avec Run Command Systems Manager

AWS Support vous fournit un document de commande d'exécution de Systems Manager pour vous interfacier avec votre instance compatible avec Systems Manager afin d'exécuter EC2Rescue pour Windows Server. Le document Exécuter la commande s'appelle `AWSSupport-RunEC2RescueForWindowsTool`.

Le document Exécuter la commande Systems Manager effectue les tâches suivantes :

- Il télécharge et vérifie EC2Rescue for Windows Server.
- Importe un PowerShell module pour faciliter votre interaction avec l'outil.
- Exécute EC2 RescueCmd avec la commande et les paramètres fournis.

Le document Exécuter la commande Systems Manager accepte trois paramètres :

- **Command** — Action EC2Rescue for Windows Server. Les valeurs autorisées actuelles sont :
 - **ResetAccess**—Réinitialise le mot de passe de l'administrateur local. Le mot de passe administrateur local de l'instance actuelle sera réinitialisé et le mot de passe généré de manière aléatoire sera stocké de manière sécurisée dans le Parameter Store en tant que `/EC2Rescue/Password/<INSTANCE_ID>`. Si vous sélectionnez cette action sans fournir de paramètres, les mots de passe sont chiffrés automatiquement avec la clé KMS par défaut. Vous pouvez aussi spécifier l'ID d'une clé KMS dans Paramètres pour chiffrer le mot de passe avec votre propre clé.
 - **CollectLogs**—Exécute EC2Rescue pour Windows Server avec l'action. `/collect:all` Si vous sélectionnez cette action, `Parameters` doit inclure le nom d'un compartiment Amazon S3 dans lequel les journaux seront chargés.
 - **FixAll**—Exécute EC2Rescue pour Windows Server avec l'action. `/rescue:all` Si vous sélectionnez cette action, `Parameters` doit inclure le nom du périphérique de stockage en mode bloc à corriger.
- **Paramètres** : PowerShell paramètres à transmettre pour la commande spécifiée.

Note

Pour que l'ResetAccessaction fonctionne, votre instance Amazon EC2 doit être associée à la politique suivante afin d'écrire le mot de passe chiffré dans Parameter Store. Attendez quelques minutes avant de tenter de réinitialiser le mot de passe d'une instance après avoir attaché cette politique au rôle IAM associé.

À l'aide de l'clé KMS par défaut :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
        Passwords/<instanceid>"
      ]
    }
  ]
}
```

À l'aide d'une clé KMS personnalisée :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
        Passwords/<instanceid>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
    "kms:Encrypt"
  ],
  "Resource": [
    "arn:aws:kms:region:account_id:key/<kmskeyid>"
  ]
}
]
```

La procédure suivante décrit comment afficher le JSON pour ce document dans la console Amazon EC2.

Pour afficher le JSON pour le document Exécuter la commande Systems Manager

1. Ouvrez la console Systems Manager à l'adresse <https://console.aws.amazon.com/systems-manager/home>.
2. Dans le panneau de navigation, développez Shared Services (Services partagés) et choisissez Documents.
3. Dans la barre de recherche, définissez Propriétaire sur M'appartenant ou appartenant à Amazon et définissez Document name prefix (Préfixe du nom du document) sur `AWSSupport-RunEC2RescueForWindowsTool`.
4. Sélectionnez le document `AWSSupport-RunEC2RescueForWindowsTool`, choisissez Contents (Contenu), puis affichez le JSON.

Exemples

Voici quelques exemples d'utilisation du document Run Command Systems Manager pour exécuter EC2Rescue pour Windows Server à l'aide de la AWS CLI. Pour plus d'informations sur l'envoi de commandes avec le AWS CLI, consultez la [référence des AWS CLI commandes](#).

Tentative de correction de tous les problèmes identifiés sur un volume racine hors connexion

Essayez de corriger tous les problèmes identifiés sur un volume racine hors connexion attaché à une instance Amazon EC2 Windows :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue offline volume xvdf" --parameters "Command=FixAll, Parameters='xvdf'" --output text
```

Collectez les journaux à partir de l'instance Amazon EC2 Windows actuelle

Collectez tous les journaux à partir de l'instance Amazon EC2 Windows en ligne actuelle et chargez-les dans un compartiment Amazon S3 :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue online log collection to S3" --parameters "Command=CollectLogs, Parameters='YOURS3BUCKETNAME'" --output text
```

Collectez les journaux à partir d'un volume d'instance Amazon EC2 Windows hors connexion

Collecter tous les journaux à partir d'un volume hors connexion vers une instance Amazon EC2 Windows et les charger dans Amazon S3 avec une URL pré-signée :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue offline log collection to S3" --parameters "Command=CollectLogs, Parameters=\"-Offline -BlockDeviceName xvdf -S3PreSignedUrl 'YOURS3PRESIGNEDURL'\"" --output text
```

Réinitialisez le mot de passe administrateur local

Les exemples suivants illustrent les méthodes vous permettant de réinitialiser le mot de passe administrateur local. La sortie fournit un lien vers Parameter Store, dans lequel vous pouvez trouver le mot de passe sécurisé généré de manière aléatoire que vous pouvez utiliser ensuite pour RDP dans votre instance Windows Amazon EC2 en tant qu'administrateur local.

Réinitialiser le mot de passe administrateur local d'une instance en ligne à l'aide de la AWS KMS key par défaut alias/aws/ssm :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters "Command=ResetAccess" --output text
```

Réinitialiser le mot de passe administrateur local d'une instance en ligne à l'aide d'une clé KMS :

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters "Command=ResetAccess, Parameters=a133dc3c-a2g4-4fc6-a873-6c0720104bf0" --output text
```

Note

Dans cet exemple, l'clé KMS est a133dc3c-a2g4-4fc6-a873-6c0720104bf0.

Console série EC2 pour instances Amazon EC2

Avec l'EC2 Serial Console , vous avez accès au port série de votre instance Amazon EC2, que vous pouvez utiliser pour résoudre les problèmes de démarrage, de configuration réseau et autres. La console série ne requiert pas que votre instance possède des capacités de mise en réseau. La console série vous permet de commander une instance comme si votre clavier et votre moniteur étaient directement connectés au port série de cette dernière. La session de la console série dure du redémarrage à l'arrêt de l'instance. Pendant le redémarrage, vous pouvez afficher tous les messages de démarrage depuis le début.

L'accès à la console série n'est pas disponible par défaut. Votre organisation doit autoriser le compte à accéder à la console série et configurer des politiques IAM pour accorder à vos utilisateurs l'accès à la console série. L'accès à la console série peut être contrôlé à un niveau granulaire à l'aide d'ID d'instance, de balises de ressources et d'autres leviers IAM. Pour plus d'informations, consultez [Configurer l'accès à l'EC2 Serial Console](#) .

Vous pouvez accéder à la console série à l'aide de la console EC2 ou de l' AWS CLI.

La console série est disponible sans frais supplémentaires.

Rubriques

- [Prérequis](#)
- [Configurer l'accès à l'EC2 Serial Console](#)
- [Connexion à l'EC2 Serial Console](#)
- [Déconnexion de l'EC2 Serial Console](#)
- [Résoudre les problèmes liés à votre instance Amazon EC2 à l'aide de la console série EC2](#)

Prérequis

Pour vous connecter à l'EC2 Serial Console et utiliser l'outil de votre choix afin de résoudre les problèmes, les conditions préalables suivantes doivent être réunies :

- [Régions AWS](#)

- [Zones Wavelength et AWS Outposts](#)
- [Zones locales](#)
- [Types d'instances](#)
- [Octroi de l'accès](#)
- [Prise en charge d'un client basé sur un navigateur](#)
- [État de l'instance](#)
- [Amazon EC2 Systems Manager](#)
- [serveur sshd](#)
- [Configuration de l'outil de dépannage de votre choix](#)

Régions AWS

Pris en charge partout Régions AWS sauf dans le Canada-Ouest (Calgary).

Zones Wavelength et AWS Outposts

Non pris en charge.

Zones locales

Prise en charge dans toutes les zones locales.

Types d'instances

Types d'instances pris en charge :

- Linux
 - Toutes les instances virtualisées créées sur la base de Nitro System.
 - Toutes les instances de matériel nu à l'exception de :
 - Usage général : a1.metal, mac1.metal, mac2.metal
 - Calcul accéléré : g5g.metal
 - Mémoire optimisée : u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal
- Windows

Toutes les instances virtualisées créées sur la base de Nitro System. Non pris en charge par les instances à matériel nu.

Octroi de l'accès

Vous devez effectuer les tâches de configuration pour octroyer l'accès à l'EC2 Serial Console. Pour plus d'informations, consultez [Configurer l'accès à l'EC2 Serial Console](#).

Prise en charge d'un client basé sur un navigateur

Pour vous connecter à la console série à [l'aide du client basé sur un navigateur](#), votre navigateur doit être compatible. WebSocket Si votre navigateur ne le prend pas en charge WebSocket, connectez-vous à la console série à [l'aide de votre propre clé et d'un client SSH](#).

État de l'instance

Doit indiquer `running`.

Vous ne pouvez pas vous connecter à la console série si l'instance est à l'état `pending`, `stopping`, `stopped`, `shutting-down` ou `terminated`.

Pour plus d'informations sur les états de l'instance, consultez [Cycle de vie d'une instance](#).

Amazon EC2 Systems Manager

Si l'instance utilise Amazon EC2 Systems Manager, SSM Agent version 3.0.854.0 ou ultérieure doit être installé sur l'instance. Pour plus d'informations sur SSM Agent, veuillez consulter [Utilisation de SSM Agent](#) dans le Guide de l'utilisateur AWS Systems Manager.

serveur sshd

Vous n'avez pas besoin qu'un serveur `sshd` soit installé ou en cours d'exécution sur votre instance.

Configuration de l'outil de dépannage de votre choix

Instances Linux

Pour dépanner votre instance Linux via la console série, vous pouvez utiliser GRUB ou SysRq. Avant de pouvoir utiliser ces outils, vous devez d'abord effectuer des étapes de configuration sur chaque instance sur laquelle vous allez les utiliser.

Outils

- [Configurer GRUB](#)
- [Configurez SysRq](#)

Configurer GRUB

Avant de pouvoir utiliser GRUB via la console série, vous devez configurer votre instance pour utiliser GRUB via la console série.

Pour configurer GRUB, choisissez l'une des procédures suivantes en fonction de l'AMI utilisée pour lancer l'instance.

Amazon Linux 2

Pour configurer GRUB sur une instance Amazon Linux 2

1. [Connectez-vous à votre instance Linux](#)
2. Ajoutez ou modifiez les options suivantes dans `/etc/default/grub`:
 - Configurez `GRUB_TIMEOUT=1`.
 - Addition `GRUB_TERMINAL="console serial"`.
 - Addition `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

Voici un exemple de `/etc/default/grub`. Vous devrez peut-être modifier la configuration en fonction de la configuration de votre système.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
  biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
GRUB_TIMEOUT=1
GRUB_DISABLE_RECOVERY="true"
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Appliquez la configuration mise à jour en exécutant la commande suivante.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Ubuntu

Pour configurer GRUB sur une instance Ubuntu

1. [Connectez-vous à votre instance.](#)

2. Ajoutez ou modifiez les options suivantes dans `/etc/default/grub.d/50-cloudimg-settings.cfg`:
 - Configurez `GRUB_TIMEOUT=1`.
 - Addition `GRUB_TIMEOUT_STYLE=menu`.
 - Addition `GRUB_TERMINAL="console serial"`.
 - Supprimez `GRUB_HIDDEN_TIMEOUT`.
 - Addition `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

Voici un exemple de `/etc/default/grub.d/50-cloudimg-settings.cfg`. Vous devrez peut-être modifier la configuration en fonction de la configuration de votre système.

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process

# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
    nvme_core.io_timeout=4294967295"

# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Appliquez la configuration mise à jour en exécutant la commande suivante.

```
[ec2-user ~]$ sudo update-grub
```

RHEL

Pour configurer GRUB sur une instance RHEL

1. [Connectez-vous à votre instance.](#)

2. Ajoutez ou modifiez les options suivantes dans `/etc/default/grub`:

- Supprimez `GRUB_TERMINAL_OUTPUT`.
- Addition `GRUB_TERMINAL="console serial"`.
- Addition `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

Voici un exemple de `/etc/default/grub`. Vous devrez peut-être modifier la configuration en fonction de la configuration de votre système.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Appliquez la configuration mise à jour en exécutant la commande suivante.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

CentOS

Pour les instances lancées à l'aide d'une AMI CentOS, GRUB est configuré pour la console série par défaut.

Voici un exemple de `/etc/default/grub`. En fonction de la configuration de votre système, il se peut que votre configuration soit différente.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
```

```
GRUB_DISABLE_RECOVERY="true"
```

Configurez SysRq

Pour configurer SysRq, vous devez activer les SysRq commandes pour le cycle de démarrage en cours. Pour que la configuration soit persistante, vous pouvez également activer les SysRq commandes pour les démarrages suivants.

Pour activer toutes les SysRq commandes pour le cycle de démarrage en cours

1. [Connectez-vous à votre instance.](#)
2. Exécutez la commande suivante.

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

Note

Ce paramètre est effacé au prochain redémarrage.

Pour activer toutes les SysRq commandes pour les démarrages suivants

1. Créez le fichier `/etc/sysctl.d/99-sysrq.conf` et ouvrez-le dans votre éditeur préféré.

```
[ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
```

2. Ajoutez la ligne suivante.

```
kernel.sysrq=1
```

3. Redémarrez l'instance pour appliquer les modifications.

```
[ec2-user ~]$ sudo reboot
```

4. À l'invite `login`, entrez le nom d'utilisateur de l'utilisateur avec un mot de passe que vous avez [configuré précédemment](#), puis appuyez sur Entrée.
5. À l'invite `Password`, entrez le mot de passe, puis appuyez sur Entrée.

instances Windows

Pour dépanner votre instance Windows via la console série, vous pouvez utiliser la console d'administration spéciale (SAC). Avant de pouvoir utiliser la SAC, vous devez d'abord activer la SAC et le menu de démarrage sur chaque instance sur laquelle vous allez l'utiliser.

Activer SAC et le menu de démarrage

Note

Si vous activez SAC sur une instance, les services EC2 qui reposent sur la récupération de mot de passe ne fonctionnent pas à partir de la console Amazon EC2. Les agents de lancement Windows on Amazon EC2 (EC2Config, EC2Launch v1 et EC2Launch v2) s'appuient sur la console série pour exécuter diverses tâches. Ces tâches ne s'exécutent pas correctement lorsque vous activez SAC sur une instance. Pour plus d'informations sur les agents de lancement de Windows sur Amazon EC2, consultez [the section called "Configuration des instances Windows"](#) Si vous activez SAC, vous pouvez le désactiver ultérieurement. Pour plus d'informations, consultez [Désactiver SAC et le menu de démarrage](#).

Utilisez l'une des méthodes suivantes pour activer SAC et le menu de démarrage sur une instance.

PowerShell

Pour activer SAC et le menu de démarrage sur une instance Windows

1. [Connectez-vous](#) à votre instance et effectuez les étapes suivantes à partir d'une ligne de PowerShell commande élevée.
2. Activez SAC.

```
bcdedit /ems '{current}' on  
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Activez le menu de démarrage.

```
bcdedit /set '{bootmgr}' displaybootmenu yes  
bcdedit /set '{bootmgr}' timeout 15  
bcdedit /set '{bootmgr}' bootems yes
```

4. Appliquez la configuration mise à jour en redémarrant l'instance.

```
shutdown -r -t 0
```

Command prompt

Pour activer SAC et le menu de démarrage sur une instance Windows

1. [Connectez-vous](#) à votre instance et exécutez les étapes suivantes à partir de l'invite de commandes.
2. Activez SAC.

```
bcdedit /ems {current} on  
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Activez le menu de démarrage.

```
bcdedit /set {bootmgr} displaybootmenu yes  
bcdedit /set {bootmgr} timeout 15  
bcdedit /set {bootmgr} bootems yes
```

4. Appliquez la configuration mise à jour en redémarrant l'instance.

```
shutdown -r -t 0
```

Configurer l'accès à l'EC2 Serial Console

Pour configurer l'accès à la console série, vous devez accorder l'accès à la console série au niveau du compte, puis configurer des politiques IAM pour accorder l'accès à vos utilisateurs. Pour les instances Linux, vous devez également configurer un utilisateur basé sur un mot de passe pour chaque instance afin que vos utilisateurs puissent utiliser la console série pour le dépannage.

Avant de commencer, assurez-vous de vérifier les [conditions préalables](#).

Rubriques

- [Niveaux d'accès à l'EC2 Serial Console](#)
- [Gérer l'accès du compte à l'EC2 Serial Console](#)
- [Configurer les politiques IAM pour l'accès à l'EC2 Serial Console](#)

- [Définir un mot de passe utilisateur du système d'exploitation sur une instance Linux](#)

Niveaux d'accès à l'EC2 Serial Console

Par défaut, il n'est pas possible d'accéder à la console série au niveau du compte. Vous devez accorder explicitement l'accès à la console série au niveau du compte. Pour plus d'informations, veuillez consulter [Gérer l'accès du compte à l'EC2 Serial Console](#).

Vous pouvez utiliser une politique de contrôle de service (SCP) pour autoriser l'accès à la console série au sein de votre organisation. Vous pouvez ensuite disposer d'un contrôle d'accès granulaire au niveau de l'utilisateur à l'aide d'une politique IAM pour contrôler l'accès. En combinant des politiques SCP et IAM, vous disposez de différents niveaux de contrôle d'accès à la console série.

Niveau de l'organisation

Vous pouvez utiliser une politique de contrôle de service (SCP) pour autoriser l'accès à la console série aux comptes membre au sein de votre organisation. Pour plus d'informations sur les SCP, veuillez consulter [Politiques de contrôle des services](#) dans le Guide de l'utilisateur AWS Organizations.

Niveau de l'instance

Vous pouvez configurer les politiques d'accès à la console série en utilisant IAM PrincipalTag et les ResourceTag constructions et en spécifiant les instances par leur ID. Pour plus d'informations, consultez [Configurer les politiques IAM pour l'accès à l'EC2 Serial Console](#).

Niveau utilisateur

Vous pouvez configurer l'accès au niveau de l'utilisateur en configurant une politique IAM pour autoriser ou interdire à un utilisateur spécifié d'envoyer la clé publique SSH en mode push au service de console série d'une instance particulière. Pour plus d'informations, consultez [Configurer les politiques IAM pour l'accès à l'EC2 Serial Console](#).

Niveau du système d'exploitation (instances Linux uniquement)

Vous pouvez définir un mot de passe utilisateur au niveau du système d'exploitation invité. Cela permet d'accéder à la console série pour certains cas d'utilisation. Toutefois, pour surveiller les journaux, vous n'avez pas besoin d'un utilisateur avec un mot de passe. Pour plus d'informations, veuillez consulter [Définir un mot de passe utilisateur du système d'exploitation sur une instance Linux](#).

Gérer l'accès du compte à l'EC2 Serial Console

Par défaut, il n'est pas possible d'accéder à la console série au niveau du compte. Vous devez accorder explicitement l'accès à la console série au niveau du compte.

Rubriques

- [Autoriser les utilisateurs à gérer l'accès du compte](#)
- [Afficher l'état de l'accès du compte à la console série](#)
- [Autoriser le compte à accéder à la console série](#)
- [Interdire au compte l'accès à la console série](#)

Autoriser les utilisateurs à gérer l'accès du compte

Pour permettre à vos utilisateurs de gérer l'accès du compte à l'EC2 Serial Console, vous devez leur octroyer les autorisations IAM requises.

La politique suivante accorde des autorisations pour afficher l'état du compte, et autoriser et interdire le compte à accéder à l'EC2 Serial Console .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:EnableSerialConsoleAccess",
        "ec2:DisableSerialConsoleAccess"
      ],
      "Resource": "*"
    }
  ]
}
```

Pour plus d'informations, consultez [Création de politiques IAM](#) dans le IAM Guide de l'utilisateur.

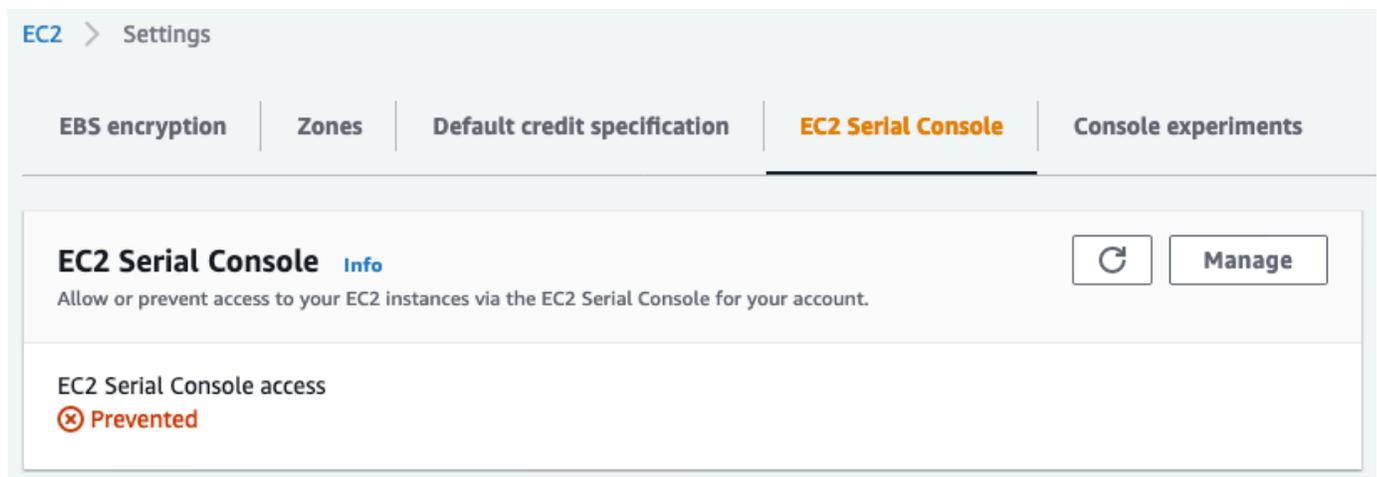
Afficher l'état de l'accès du compte à la console série

Pour afficher l'état de l'accès du compte à la console série (console)

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, sélectionnez EC2 Dashboard (Tableau de bord EC2).
3. Dans Attributs du compte, choisissez EC2 Serial Console .

Le champ EC2 Serial Console access (Accès à l'EC2 Serial Console) indique si l'accès du compte est Allowed (Autorisé) ou Prevented (Bloqué).

La capture d'écran suivante montre que le compte n'est pas autorisé à utiliser l'EC2 Serial Console .



Pour afficher l'état d'accès du compte à la console série (AWS CLI)

Utilisez la commande [get-serial-console-access-status](#) pour afficher l'état d'accès du compte à la console série.

```
aws ec2 get-serial-console-access-status --region us-east-1
```

Dans le résultat suivant, `true` indique que le compte est autorisé à accéder à la console série.

```
{  
  "SerialConsoleAccessEnabled": true  
}
```

Autoriser le compte à accéder à la console série

Pour autoriser le compte à accéder à la console série (console)

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, sélectionnez EC2 Dashboard (Tableau de bord EC2).
3. Dans Attributs du compte, choisissez EC2 Serial Console .
4. Choisissez Gérer.
5. Pour autoriser toutes les instances du compte à accéder à l'EC2 Serial Console , cochez la case Autoriser.
6. Sélectionnez Mise à jour.

Pour autoriser le compte à accéder à la console série (AWS CLI)

Utilisez la commande [enable-serial-console-access](#) pour autoriser le compte à accéder à la console série.

```
aws ec2 enable-serial-console-access --region us-east-1
```

Dans le résultat suivant, `true` indique que le compte est autorisé à accéder à la console série.

```
{  
  "SerialConsoleAccessEnabled": true  
}
```

Interdire au compte l'accès à la console série

Pour interdire au compte l'accès à la console série (console)

1. Ouvrez la console Amazon EC2 sur <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation de gauche, sélectionnez EC2 Dashboard (Tableau de bord EC2).
3. Dans Attributs du compte, choisissez EC2 Serial Console .
4. Choisissez Gérer.
5. Pour interdire l'accès à l'EC2 Serial Console à toutes les instances du compte, décochez Autoriser.
6. Sélectionnez Mise à jour.

Pour interdire au compte l'accès à la console série (AWS CLI)

Utilisez la commande [disable-serial-console-access](#) pour interdire au compte l'accès à la console série.

```
aws ec2 disable-serial-console-access --region us-east-1
```

Dans le résultat suivant, `false` indique que le compte n'est pas autorisé à accéder à la console série.

```
{
  "SerialConsoleAccessEnabled": false
}
```

Configurer les politiques IAM pour l'accès à l'EC2 Serial Console

Par défaut, vos utilisateurs n'ont pas accès à la console série. Votre organisation doit configurer des politiques IAM pour accorder à vos utilisateurs l'accès requis. Pour plus d'informations, consultez [Création de politiques IAM](#) dans le IAM Guide de l'utilisateur.

Pour accéder à la console série, créez un document de politique JSON qui inclut l'action `ec2-instance-connect:SendSerialConsoleSSHPublicKey`. Cette action accorde à un utilisateur l'autorisation d'envoyer la clé publique en mode push au service de console série, qui démarre une session de console série. Nous vous recommandons de limiter l'accès à des instances EC2 spécifiques. Sinon, tous les utilisateurs disposant de cette autorisation peuvent se connecter à la console série de toutes les instances EC2.

Exemple de politiques IAM

- [Autoriser explicitement l'accès à la console série](#)
- [Refuser explicitement l'accès à la console série](#)
- [Utiliser des balises de ressources pour contrôler l'accès à la console série](#)

Autoriser explicitement l'accès à la console série

Par défaut, personne n'a accès à la console série. Pour accorder l'accès à la console série, vous devez configurer une politique pour autoriser explicitement cet accès. Nous vous recommandons de configurer une politique qui restreint l'accès à des instances spécifiques.

La politique suivante permet d'accéder à la console série d'une instance spécifique, identifiée par son ID d'instance.

Notez que les actions `DescribeInstances`, `DescribeInstanceTypes` et `GetSerialConsoleAccessStatus` ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, toutes les ressources, indiquées par un astérisque *, doivent être spécifiées pour ces actions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribeInstances",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:GetSerialConsoleAccessStatus"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowinstanceBasedSerialConsoleAccess",
      "Effect": "Allow",
      "Action": [
        "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
      ],
      "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
    }
  ]
}
```

Refuser explicitement l'accès à la console série

La politique IAM suivante autorise l'accès à la console série de toutes les instances, désignées par * (astérisque), et refuse explicitement l'accès à la console série d'une instance spécifique, identifiée par son ID.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Sid": "AllowSerialConsoleAccess",
    "Effect": "Allow",
    "Action": [
        "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:GetSerialConsoleAccessStatus"
    ],
    "Resource": "*"
  },
  {
    "Sid": "DenySerialConsoleAccess",
    "Effect": "Deny",
    "Action": [
        "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
    ],
    "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
  }
]
}

```

Utiliser des balises de ressources pour contrôler l'accès à la console série

Vous pouvez utiliser des balises de ressource pour contrôler l'accès à la console série d'une instance.

Le contrôle d'accès basé sur les attributs est une stratégie d'autorisation qui définit les autorisations en fonction de balises pouvant être associées aux utilisateurs et AWS aux ressources. Par exemple, la politique suivante permet à un utilisateur d'initier une connexion à la console série pour une seule instance si la balise de ressource de cette instance et la balise du principal possèdent la même valeur `SerialConsole` en clé de balise.

Pour plus d'informations sur l'utilisation de balises pour contrôler l'accès à vos AWS ressources, consultez la section [Contrôle de l'accès aux AWS ressources](#) dans le guide de l'utilisateur IAM.

Notez que les actions `DescribeInstances`, `DescribeInstanceTypes` et `GetSerialConsoleAccessStatus` ne prennent pas en charge les autorisations au niveau des ressources. Par conséquent, toutes les ressources, indiquées par un astérisque `*`, doivent être spécifiées pour ces actions.

```

{
  "Version": "2012-10-17",

```

```

"Statement": [
  {
    "Sid": "AllowDescribeInstances",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceTypes",
      "ec2:GetSerialConsoleAccessStatus"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowTagBasedSerialConsoleAccess",
    "Effect": "Allow",
    "Action": [
      "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
    ],
    "Resource": "arn:aws:ec2:region:account-id:instance/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/SerialConsole":
"${aws:PrincipalTag/SerialConsole}"
      }
    }
  }
]
}

```

Définir un mot de passe utilisateur du système d'exploitation sur une instance Linux

Note

Cette section s'applique uniquement aux instances Linux.

Vous pouvez vous connecter à la console série sans mot de passe. Toutefois, pour utiliser la console série pour le dépannage d'une instance Linux, celle-ci doit disposer d'un utilisateur du système d'exploitation basé sur un mot de passe.

Vous pouvez définir le mot de passe pour n'importe quel utilisateur du système d'exploitation, y compris l'utilisateur racine. Notez que l'utilisateur racine peut modifier tous les fichiers, tandis que chaque utilisateur du système d'exploitation peut avoir des autorisations limitées.

Vous devez définir un mot de passe utilisateur pour chaque instance pour laquelle vous utilisez la console série. Vous n'aurez besoin d'effectuer cette opération qu'une seule fois pour chaque instance.

Note

Les instructions suivantes ne s'appliquent que si vous avez lancé votre instance à l'aide d'une AMI Linux fournie par AWS car, par défaut, les AMI fournies par ne AWS sont pas configurées avec un utilisateur basé sur un mot de passe. Si vous avez lancé votre instance à l'aide d'une AMI sur laquelle le mot de passe utilisateur racine est déjà configuré, vous pouvez ignorer ces instructions.

Pour définir un mot de passe utilisateur du système d'exploitation sur une instance Linux

1. [Connectez-vous à votre instance](#). Vous pouvez utiliser n'importe quelle méthode de connexion à votre instance, à l'exception de la méthode de connexion à l'EC2 Serial Console .
2. Pour définir le mot de passe d'un utilisateur, utilisez la commande `passwd`. Dans l'exemple suivant, l'utilisateur est `root`.

```
[ec2-user ~]$ sudo passwd root
```

Voici un exemple de sortie.

```
Changing password for user root.  
New password:
```

3. À l'invite `New password`, entrez le nouveau mot de passe.
4. À l'invite, saisissez à nouveau le mot de passe.

Connexion à l'EC2 Serial Console

Vous pouvez vous connecter à la console série de votre instance EC2 à l'aide de la console Amazon EC2 ou via SSH. Une fois connecté à la console série, vous pouvez l'utiliser pour résoudre les problèmes de démarrage, de configuration réseau et autres. Pour plus d'informations sur la résolution des problèmes, consultez [Résoudre les problèmes liés à votre instance Amazon EC2 à l'aide de la console série EC2](#).

Considérations

- Une seule connexion de console série active est prise en charge par instance.
- La connexion à la console série dure généralement une heure, à moins que vous ne vous déconnectiez. Toutefois, pendant la maintenance du système, Amazon EC2 déconnecte la session de console série.
- 30 secondes sont nécessaires pour déconnecter une session après la déconnexion de la console série afin d'autoriser une nouvelle session.
- Ports de console série pris en charge : `ttys0` (instances Linux) et `COM1` (instances Windows)
- Lorsque vous vous connectez à la console série, vous pouvez observer une légère baisse de débit de votre instance.

Rubriques

- [Connexion à l'aide du client basé sur un navigateur](#)
- [Connexion à l'aide de votre propre clé et d'un client SSH](#)
- [Points de terminaison et empreintes digitales de l'EC2 Serial Console](#)

Connexion à l'aide du client basé sur un navigateur

Vous pouvez vous connecter à la console série de votre instance EC2 à l'aide du client basé sur le navigateur. Pour ce faire, sélectionnez l'instance sur la console Amazon EC2 et choisissez de vous connecter à la console série. Le client basé sur le navigateur gère les autorisations et fournit une connexion réussie.

L'EC2 Serial Console fonctionne à partir de la plupart des navigateurs et prend en charge les entrées au clavier et à la souris.

Avant d'établir la connexion, assurez-vous d'avoir réuni les [conditions préalables](#).

Pour vous connecter au port série de votre instance à l'aide du client basé sur le navigateur (console Amazon EC2)

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Instances.
3. Sélectionnez l'instance et choisissez Actions, Monitor and troubleshoot (Surveiller et dépanner), EC2 Serial Console, Connect (Se connecter).

Sinon, sélectionnez l'instance et choisissez Connect (Se connecter), EC2 Serial Console, Connect (Se connecter).

Une fenêtre de terminal dans le navigateur s'ouvre.

- Appuyez sur Entrée. Si une invite de connexion est retournée, vous êtes connecté à la console série.

Si l'écran reste noir, vous pouvez utiliser les informations suivantes pour résoudre les problèmes de connexion à la console série :

- Vérifiez que vous avez configuré l'accès à la console série. Pour plus d'informations, consultez [Configurer l'accès à l'EC2 Serial Console](#).
- (Instances Linux uniquement) SysRq À utiliser pour se connecter à la console série. SysRq ne nécessite pas que vous vous connectiez via le client basé sur un navigateur. Pour plus d'informations, consultez [Résolvez les problèmes de votre instance Linux à l'aide de SysRq](#).
- (Instances Linux uniquement) Redémarrez getty. Si vous disposez d'un accès SSH à votre instance, connectez-vous à cette dernière à l'aide de SSH et redémarrez getty à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
```

- Redémarrez votre instance. Vous pouvez redémarrer votre instance en utilisant SysRq (instances Linux), la console EC2 ou le AWS CLI. Pour plus d'informations, consultez [Résolvez les problèmes de votre instance Linux à l'aide de SysRq](#) (instances Linux) ou [Redémarrer votre instance](#).
- (Instances Linux uniquement) À l'**login**invite, entrez le nom d'utilisateur de l'utilisateur basé sur un mot de passe que vous avez [configuré précédemment](#), puis appuyez sur Entrée.
 - (Instances Linux uniquement) À l'**Password**invite, entrez le mot de passe, puis appuyez sur Entrée.

Vous êtes maintenant connecté à l'instance et pouvez utiliser la console série pour résoudre les problèmes.

Connexion à l'aide de votre propre clé et d'un client SSH

Vous pouvez utiliser votre propre clé SSH et vous connecter à votre instance à partir du client SSH de votre choix en utilisant l'API de la console série. Vous bénéficiez ainsi de la capacité de la console série d'envoyer une clé publique en mode push à l'instance.

Avant d'établir la connexion, assurez-vous d'avoir réuni les [conditions préalables](#).

Pour vous connecter à la console série d'une instance à l'aide de SSH

1. Envoyez votre clé publique SSH en mode push à l'instance pour démarrer une session de console série

Utilisez la commande [send-serial-console-ssh-public-key](#) pour envoyer votre clé publique SSH en mode push à l'instance. Une session de console série démarre.

Si une session de console série a déjà été démarrée pour cette instance, la commande échoue car vous ne pouvez avoir qu'une seule session ouverte à la fois. 30 secondes sont nécessaires pour déconnecter une session après la déconnexion de la console série afin d'autoriser une nouvelle session.

```
aws ec2-instance-connect send-serial-console-ssh-public-key \  
  --instance-id i-001234a4bf70dec41EXAMPLE \  
  --serial-port 0 \  
  --ssh-public-key file://my_key.pub \  
  --region us-east-1
```

2. Connexion à la console série à l'aide de votre clé privée

Utilisez la commande `ssh` pour vous connecter à la console série avant que la clé publique ne soit supprimée du service de console série. Vous avez 60 secondes avant sa suppression.

Utilisez la clé privée qui correspond à la clé publique.

Le format du nom d'utilisateur est `instance-id.port0`. Il comprend l'ID d'instance et le port 0. Dans l'exemple suivant, le nom d'utilisateur est `i-001234a4bf70dec41EXAMPLE.port0`.

Le point de terminaison du service Serial Console est différent pour chaque région. Consultez le tableau [Points de terminaison et empreintes digitales de l'EC2 Serial Console](#) pour le point de terminaison de chaque région. Dans l'exemple suivant, le service de console série se trouve dans la région *us-east-1*.

```
ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
```

3. (Facultatif) Vérification de l'empreinte digitale

Lorsque vous vous connectez pour la première fois à la console série, vous êtes invité à vérifier l'empreinte digitale. Vous pouvez comparer l'empreinte digitale de la console série avec l'empreinte digitale affichée pour vérification. Si ces empreintes ne correspondent pas, quelqu'un essaie peut-être d'effectuer une attaque MITM. Si elles correspondent, vous pouvez vous connecter en toute confiance à la console série.

L'empreinte digitale suivante concerne le service de console série dans la région us-east-1. Pour obtenir les empreintes digitales de chaque région, consultez [Points de terminaison et empreintes digitales de l'EC2 Serial Console](#).

```
SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
```

Note

L'empreinte digitale n'apparaît que la première fois que vous vous connectez à la console série.

4. Appuyez sur Entrée. Si une invite est retournée, vous êtes connecté à la console série.

Si l'écran reste noir, vous pouvez utiliser les informations suivantes pour résoudre les problèmes de connexion à la console série :

- Vérifiez que vous avez configuré l'accès à la console série. Pour plus d'informations, consultez [Configurer l'accès à l'EC2 Serial Console](#).
- (Instances Linux uniquement) SysRq À utiliser pour se connecter à la console série. SysRq ne nécessite pas de connexion via SSH. Pour plus d'informations, consultez [Résolvez les problèmes de votre instance Linux à l'aide de SysRq](#).
- (Instances Linux uniquement) Redémarrez getty. Si vous disposez d'un accès SSH à votre instance, connectez-vous à cette dernière à l'aide de SSH et redémarrez getty à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
```

- Redémarrez votre instance. Vous pouvez redémarrer votre instance en utilisant SysRq (instances Linux uniquement), la console EC2 ou le AWS CLI. Pour plus d'informations, consultez [Résolvez les problèmes de votre instance Linux à l'aide de SysRq](#) (instances Linux uniquement) ou [Redémarrer votre instance](#).
5. (Instances Linux uniquement) À l'**login**invite, entrez le nom d'utilisateur de l'utilisateur basé sur un mot de passe que vous avez [configuré précédemment](#), puis appuyez sur Entrée.
 6. (Instances Linux uniquement) À l'**Password**invite, entrez le mot de passe, puis appuyez sur Entrée.

Vous êtes maintenant connecté à l'instance et pouvez utiliser la console série pour résoudre les problèmes.

Points de terminaison et empreintes digitales de l'EC2 Serial Console

Vous trouverez ci-dessous les points de terminaison de service et les empreintes digitales de l'EC2 Serial Console. Pour vous connecter par programmation à la Serial Console d'une instance, vous utilisez un point de terminaison EC2 Serial Console. Les points de terminaison EC2 Serial Console sont uniques pour chaque Région AWS .

Nom de la région	Région	Point de terminaison	Empreinte digitale
USA Est (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256 : EhWPk TzRt TY7TRSzz2 6xBB0/HVV 9JRM7MCZN0XW/ D/0
US East (Virginie du Nord)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256 DiJa : DXWN5mA/X ADVMeBZgE rU5L2GX+Yi5L LUCz0FMMW
USA Ouest (Californie du Nord)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256:OH IdlcMET8u 7QLSX3jmR

Nom de la région	Région	Point de terminaison	Empreinte digitale
			TRAPFHVtq byoLZBMUCqiH3Y
USA Ouest (Oregon)	us-west-2	serial-console.ec2- instance-connect.us- west-2.aws	SHA256 : EMCle23 Bi6yG DHHavha1O 2JXVUC TqKa HainqZc MwqNk
Afrique (Le Cap)	af-south-1	ec2-serial-console.af- south-1.api.aws	SHA256 : RMWWZ2F JuQZJO5JL2K HLZ21ED00BlWi VePe IgXsczo
Asie-Pacifique (Hong Kong)	ap-east-1	ec2-serial-console.ap- east-1.api.aws	SHA256 : T0Q1LPi Z P7TKM2XXVIC9BJ XxCho HplnAkjb FsjYnifk
Asie-Pacifique (Hyderabad)	ap-south-2	ec2-serial-console.ap- south-2.api.aws	SHA256 : WJGPBSWV4/SHN +OPit YJ15DVW84 5JEHDKRS ValoewAu
Asie-Pacifique (Jakarta)	ap-southeast-3	ec2-serial-console.ap- southeast-3.api.aws	SHA 256 : 5 +LFNS32XI TQL/4O0ZI FBX4BZGSY FQY3O8MIK ZwgrCh
Asie-Pacifique (Melbourne)	ap-southeast-4	ec2-serial-console.ap- southeast-4.api.aws	SHA256 FgLvjn : Avaq27h 5GTSSHZ0O V7H90P0GG 46Wfoet6ZJVM

Nom de la région	Région	Point de terminaison	Empreinte digitale
Asie-Pacifique (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256 : OBL HHEBLIA H8ISO51RE ZTPISM35BSU40 XcYmklq RxEg
Asie-Pacifique (Osaka)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256 BnBu FnHr : AM0/JIBK 9AXSGEV3G8TU/ VVHFXE/3UCYJSQ
Asie-Pacifique (Séoul)	ap-northeast-2	serial-console.ec2-instance-connect.ap-northeast-2.aws	SHA256:FoqWXNX +DZ++GuNTztg9 PK49WYMqBX +FrcZM2dSrql
Asie-Pacifique (Singapour)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256 QgZua : PLFNN7WNC QDHX3QMWLU1Gy/ O8TUX7L C6L45COY
Asie-Pacifique (Sydney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256 FvMw : Y UK9LEUQJQ TRoxXZUN+CW9/ VSE9W984CF5TGZ o4
Asie-Pacifique (Tokyo)	ap-northeast-1	serial-console.ec2-instance-connect.ap-northeast-1.aws	SHA256 OfQawew : RQFSDCZT TRDV1T9EM /HMRFQE+C rliOT5uM4K

Nom de la région	Région	Point de terminaison	Empreinte digitale
Canada (Centre)	ca-central-1	serial-console.ec2- instance-connect.ca- central-1.aws	SHA256 : P2O2JO O6YW738Fiothdu 2GCzymm7S4 ZwmpMwkp TyEv
Chine (Beijing)	cn-north-1	ec2-serial-console .cn-north-1.api.am azonwebsiteservices.co m.cn	SHA 256 : 2 GHVfy4H7U U3+WAFUXD28V/gg LGGT+Y MeqjvSlgn gpg
Chine (Ningxia)	cn-northwest-1	ec2-serial-console .cn-northwest-1.ap i.amazonwebservice s.com.cn	SHA256 OdVf : TDGRNZKiQ YeBuHo4SZ UA09VWi5RYOZG en GPWMIM
Europe (Francfort)	eu-central-1	serial-console.ec2- instance-connect.eu- central-1.aws	SHA256 IcOd OikXv : ACMFS/ Y OL8AMZ1TO E+BBNRJJ3 FY0K0DE2C
Europe (Irlande)	eu-west-1	serial-console.ec2- instance-connect.eu- west-1.aws	SHA256 TrHj : H2AAGAWO4 HathHTM6E ZS3BJ7UDGUXi2Q ZAwCW6E
Europe (Londres)	eu-west-2	serial-console.ec2- instance-connect.eu- west-2.aws	SHA256 RnJg : A69RD5CE/ AEG4AMM53 I6LKD1ZPVS/ BCV3TTPW2 8

Nom de la région	Région	Point de terminaison	Empreinte digitale
Europe (Milan)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256 JnpgFy : LC0KOv BvRXN0A7N 99ECLBXSX 95CUUS7x7QK30
Europe (Paris)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:q8ldnAf9pym eNe8BnFVngY3RPAr/ kxswJUzfrlxeEWs
Europe (Espagne)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256 NxqFx : GOCW2DFRL U669Q ECSR6FZUZ /4F4N7T45 ZcwoEc
Europe (Stockholm)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256 DvocDi : TKGFFuVu GSS3Cu8GD L6W2UI32E PNPKFKLWX84
Europe (Zurich)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA 256 : 8 PPx2mbmF6 0N WdCw M4/4oAxFU TqxWp6MK UlzKfw IfRz
Israël (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256 NvtYy : JR6Q8V6KN NPI8+QSFQ 4DJ5DimNM ZPTGWGSM1S U

Nom de la région	Région	Point de terminaison	Empreinte digitale
Moyen-Orient (Bahreïn)	me-south-1	ec2-serial-console .me-south-1.api.aws	SHA256 QnLd : NPJLLKHU2 UQ2kVarso K5xVpJOMr JKCBZCDQC3K8
Moyen-Orient (EAU)	me-central-1	ec2-serial-console .me-central-1.api.aws	SHA256 FwPeyyk : ZPB5DUKIBZ+L0D B4MP par Hi/XZXNEF SDKBVLE
Amérique du Sud (São Paulo)	sa-east-1	serial-console.ec2- instance-connect.sa- east-1.aws	SHA256 NaQz : RD2+/32ognjew1yvie me C+botBiH6 2OQAPDQ1DI
AWS GovCloud (USA Est)	us-gov-east-1	serial-console.ec2 -instance-connect. us-gov-east-1.amaz onaws.com	SHA256 IkqnDc : TiWe19GWS oyLCLRTVU38YEEH +DH ZNMTeBVF28
AWS GovCloud (US-Ouest)	us-gov-west-1	serial-console.ec2 -instance-connect. us-gov-west-1.amaz onaws.com	SHA256 : KFOFRWLAOZFB +UTBD3BRF8 8NgO2YZLQx 5DQ OIPf Zilw

Déconnexion de l'EC2 Serial Console

Si vous n'avez plus besoin d'être connecté à l'EC2 Serial Console de votre instance, vous pouvez vous en déconnecter. Lorsque vous vous déconnectez de la console série, toutes les sessions shell en cours d'exécution sur l'instance continuent de s'exécuter. Si vous souhaitez mettre fin à la session du shell, vous devez y mettre fin avant de vous déconnecter de la console série.

Considérations

- La connexion à la console série dure généralement une heure, à moins que vous ne vous déconnectiez. Toutefois, pendant la maintenance du système, Amazon EC2 déconnecte la session de console série.
- 30 secondes sont nécessaires pour déconnecter une session après la déconnexion de la console série afin d'autoriser une nouvelle session.

La méthode de déconnexion de la console série dépend du client.

Client basé sur le navigateur

Pour vous déconnecter de la console série, fermez la fenêtre du terminal du navigateur de la console.

Client OpenSSH standard

Pour vous déconnecter de la console série, utilisez la commande suivante pour fermer la connexion SSH. Cette commande doit être exécutée immédiatement après une nouvelle ligne.

```
~.
```

La commande permettant d'interrompre une connexion SSH peut être différente selon le client SSH que vous utilisez.

Résoudre les problèmes liés à votre instance Amazon EC2 à l'aide de la console série EC2

À l'aide de l'EC2 Serial Console, vous pouvez résoudre les problèmes de démarrage, de configuration réseau et autres en vous connectant au port série de votre instance.

Note

Avant de commencer, assurez-vous d'avoir rempli les [prérequis](#).

Instances Linux

Rubriques

- [Résolution des problèmes de votre instance Linux à l'aide de GRUB](#)
- [Résolvez les problèmes de votre instance Linux à l'aide de SysRq](#)

Résolution des problèmes de votre instance Linux à l'aide de GRUB

GNU GRUB (abréviation de GNU GRand Unified Bootloader, communément appelé GRUB) est le chargeur de démarrage par défaut pour la plupart des systèmes d'exploitation Linux. Dans le menu GRUB, vous pouvez sélectionner le noyau dans lequel démarrer ou modifier les entrées du menu pour modifier le mode de démarrage du noyau. Cela peut être utile lors de la résolution des problèmes d'une instance défaillante.

Le menu GRUB s'affiche pendant le processus de démarrage. Le menu n'est pas accessible via le SSH normal, mais vous pouvez y accéder via l'EC2 Serial Console .

Single user mode

Le mode utilisateur unique démarre le noyau à un niveau d'exécution inférieur. Par exemple, il peut monter le système de fichiers mais pas activer le réseau, ce qui vous permet d'effectuer la maintenance nécessaire pour réparer l'instance.

Pour démarrer en mode utilisateur unique

1. [Connectez-vous](#) à la console série de l'instance.
2. Redémarrez l'instance à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo reboot
```

3. Pendant le redémarrage, lorsque le menu GRUB apparaît, appuyez sur n'importe quelle touche pour arrêter le processus de démarrage.
4. Dans le menu GRUB, utilisez les touches fléchées pour sélectionner le noyau de démarrage et appuyez sur **e** sur votre clavier.
5. Utilisez les touches fléchées pour localiser votre curseur sur la ligne contenant le noyau. La ligne commence par `linux` ou `linux16` en fonction de l'AMI utilisée pour lancer l'instance. Pour Ubuntu, deux lignes commençant par `linux` doivent toutes deux être modifiées à l'étape suivante.
6. À la fin de la ligne, ajoutez le mot `single`.

Voici un exemple pour Amazon Linux 2.

```
linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
dadd-4499-938d-ebbf42c3e499 ro console=tty0 console=ttyS0,115200n8 net.ifname\
s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
ll=0 single
```

7. Appuyez sur Ctrl+X pour démarrer en mode utilisateur unique.
8. À l'invite login, entrez le nom d'utilisateur de l'utilisateur avec un mot de passe que vous avez [configuré précédemment](#), puis appuyez sur Entrée.
9. À l'invite Password, entrez le mot de passe, puis appuyez sur Entrée.

Emergency mode

Le mode d'urgence est similaire au mode utilisateur unique, sauf que le noyau fonctionne au niveau d'exécution le plus bas possible.

Pour démarrer en mode d'urgence, suivez les mêmes étapes que le mode utilisateur unique, mais à l'étape 6, ajoutez le mot à la emergency place desingle.

Résolvez les problèmes de votre instance Linux à l'aide de SysRq

La touche System Request (SysRq), parfois qualifiée de SysRq « magique », peut être utilisée pour envoyer directement une commande au noyau, en dehors d'un shell, et le noyau répondra, indépendamment de ce que fait le noyau. Par exemple, si l'instance ne répond plus, vous pouvez utiliser la SysRq clé pour indiquer au noyau de se bloquer ou de redémarrer. Pour plus d'informations, voir [Magic SysRq key](#) sur Wikipedia.

Vous pouvez utiliser des SysRq commandes dans le client basé sur le navigateur de la console série EC2 ou dans un client SSH. La commande d'envoi d'une requête d'interruption est différente pour chaque client.

Pour l'utiliser SysRq, choisissez l'une des procédures suivantes en fonction du client que vous utilisez.

Browser-based client

À utiliser SysRq dans le client basé sur le navigateur de la console série

1. [Connectez-vous](#) à la console série de l'instance.

2. Pour envoyer une demande d'interruption, appuyez sur CTRL+0 (zéro). Si votre clavier prend cette fonctionnalité en charge, vous pouvez également envoyer une demande d'interruption à l'aide de la touche Pause ou Attn.

```
[ec2-user ~]$ CTRL+0
```

3. Pour émettre une SysRq commande, appuyez sur la touche de votre clavier correspondant à la commande requise. Par exemple, pour afficher une liste de SysRq commandes, appuyez sur h.

```
[ec2-user ~]$ h
```

Le résultat de la commande h est similaire à ce qui suit.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

SSH client

À utiliser SysRq dans un client SSH

1. [Connectez-vous](#) à la console série de l'instance.
2. Pour envoyer une demande d'interruption, appuyez sur ~B (tilde, suivi de B majuscule).

```
[ec2-user ~]$ ~B
```

3. Pour émettre une SysRq commande, appuyez sur la touche de votre clavier correspondant à la commande requise. Par exemple, pour afficher une liste de SysRq commandes, appuyez sur h.

```
[ec2-user ~]$ h
```

Le résultat de la commande h est similaire à ce qui suit.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-  
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems  
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-  
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r  
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-  
buffer(z)
```

Note

La commande permettant d'envoyer une requête d'interruption peut être différente selon le client SSH que vous utilisez.

instances Windows

Utiliser SAC pour résoudre les problèmes de votre instance Windows

La console d'administration spéciale (SAC) de Windows permet de résoudre les problèmes d'une instance Windows. En vous connectant à la console série de l'instance et en utilisant SAC, vous pouvez interrompre le processus de démarrage et démarrer Windows en mode sans échec.

Note

Si vous activez SAC sur une instance, les services EC2 qui reposent sur la récupération de mot de passe ne fonctionnent pas à partir de la console Amazon EC2. Les agents de lancement Windows on Amazon EC2 (EC2Config, EC2Launch v1 et EC2Launch v2) s'appuient sur la console série pour exécuter diverses tâches. Ces tâches ne s'exécutent pas correctement lorsque vous activez SAC sur une instance. Pour plus d'informations sur les agents de lancement de Windows sur Amazon EC2, consultez [the section called "Configuration des instances Windows"](#) Si vous activez SAC, vous pouvez le désactiver ultérieurement. Pour plus d'informations, consultez [Désactiver SAC et le menu de démarrage](#).

Rubriques

- [Utiliser SAC](#)
- [Utiliser le menu de démarrage](#)
- [Désactiver SAC et le menu de démarrage](#)

Utiliser SAC

Pour utiliser SAC

1. [Connectez-vous à la console série](#)

Si SAC est activée sur l'instance, la console série affiche l'invite SAC>.

```
Computer is booting, SAC started and initialized.

Use the "ch -?" command for information about using channels.
Use the "?" command for general help.

SAC>?
EVENT: The CMD command is now available.
SAC_
```

2. Pour afficher les commandes SAC, saisissez ?, puis appuyez sur Entrée.

Sortie attendue

```
SAC>?
ch          Channel management commands. Use ch -? for more help.
cmd        Create a Command Prompt channel.
d          Dump the current kernel log.
f          Toggle detailed or abbreviated tlist info.
? or help  Display this list.
i          List all IP network numbers and their IP addresses.
i <#> <ip> <subnet> <gateway> Set IPv4 addr., subnet and gateway.
id         Display the computer identification information.
k <pid>    Kill the given process.
l <pid>    Lower the priority of a process to the lowest possible.
lock      Lock access to Command Prompt channels.
m <pid> <MB-allow> Limit the memory usage of a process to <MB-allow>.
p         Toggle paging the display.
r <pid>    Raise the priority of a process by one.
s         Display the current time and date (24 hour clock used).
s mm/dd/yyyy hh:mm Set the current time and date (24 hour clock used).
t         Tlist.
restart    Restart the system immediately.
shutdown   Shutdown the system immediately.
crashdump  Crash the system. You must have crash dump enabled.
```

3. Pour créer un canal d'invite de commandes (tel que cmd0001 ou cmd0002), saisissez **cmd**, puis appuyez sur Entrée.

4. Pour afficher le canal d'invite de commande, appuyez sur ÉCHAP, puis appuyez sur TAB.

Sortie attendue

```
Name:          Cmd0001
Description:   Command
Type:         VT-UTF8
Channel GUID:  ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Pour changer de canal, appuyez simultanément sur ÉCHAP + TAB + numéro de canal. Par exemple, pour basculer vers le canal cmd0002 (s'il a été créé), appuyez sur ÉCHAP+Tab+2.
6. Entrez les informations d'identification requises par le canal d'invite de commandes.

```
Please enter login credentials.
Username: Administrator
Domain : .
Password: *****
```

L'invite de commande correspond au shell de commande complet que vous obtenez sur un bureau, mais ne permet toutefois pas la lecture des caractères déjà envoyés.

```
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
On computer: EC2AMAZ-ASR4SAI

DISKPART> list disk

   Disk ###  Status              Size               Free               Dyn  Gpt
   -----  -
   Disk 0    Online              30 GB               0 B
   Disk 1    Online              46 GB              46 GB

DISKPART>
```

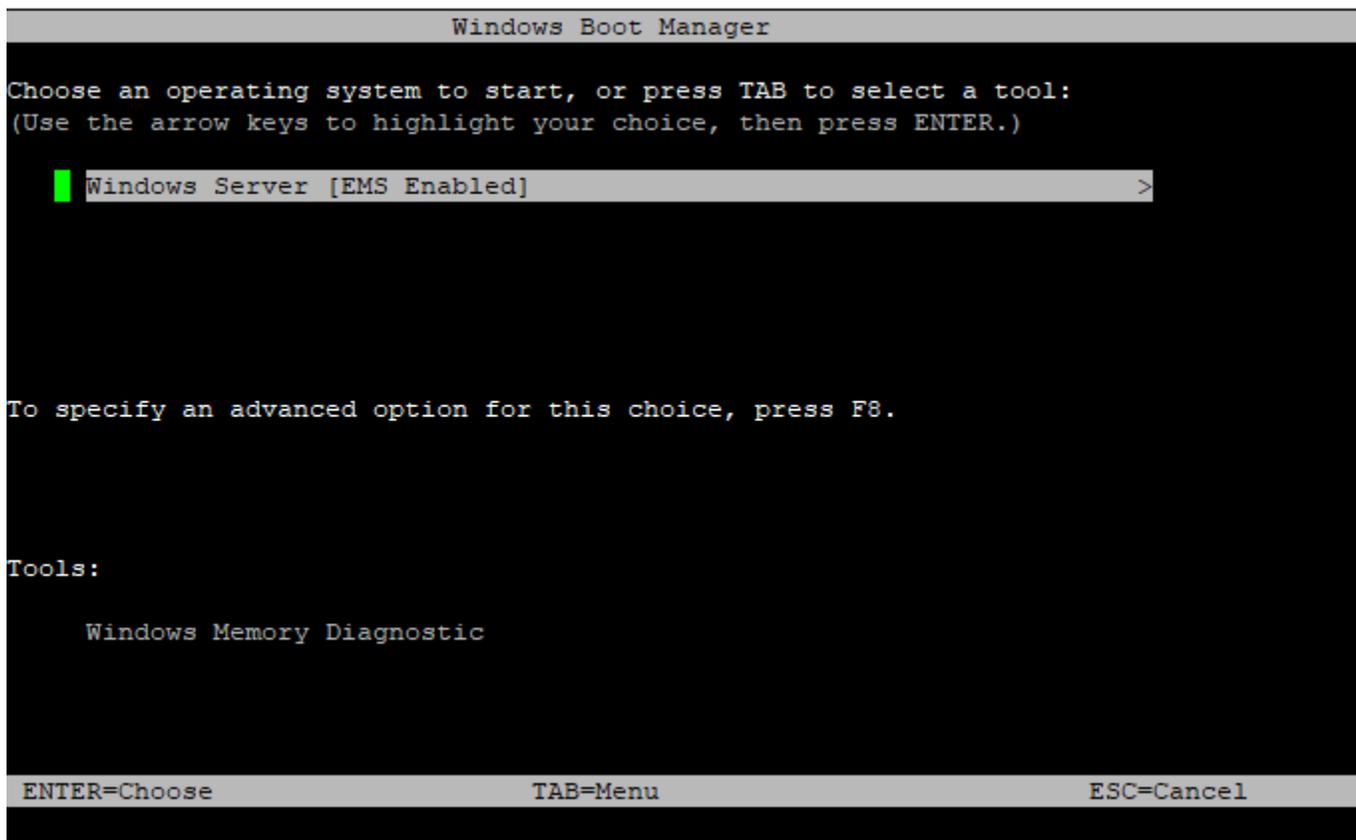
PowerShell peut également être utilisé à partir de l'invite de commande.

Notez que vous devrez peut-être définir la préférence de progression en mode silencieux.

```
PS C:\Windows\system32> $ProgressPreference="SilentlyContinue"
PS C:\Windows\system32> $computerInfo = Get-ComputerInfo
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Name
Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Description
Intel64 Family 6 Model 85 Stepping 4
PS C:\Windows\system32> _
```

Utiliser le menu de démarrage

Si le menu de démarrage de l'instance est activé et qu'il est redémarré après la connexion via SSH, vous devriez voir le menu de démarrage, comme suit.



Commandes du menu de démarrage

ENTRÉE

Démarre l'entrée sélectionnée du système d'exploitation.

TAB

Bascule vers le menu Outils.

ESC

Annule et redémarre l'instance.

ESC suivi de 8

Revient à appuyer sur F8. Affiche les options avancées de l'élément sélectionné.

Touche Esc + flèche gauche

Retourne au menu de démarrage initial.

Note

La touche Esc seule ne vous ramène pas au menu principal car Windows attend de voir si une séquence d'échappement est en cours.

```
Advanced Boot Options

Choose Advanced Options for: Windows Server
(Use the arrow keys to highlight your choice.)

Repair Your Computer

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot Logging
Enable low-resolution video
Last Known Good Configuration (advanced)
Debugging Mode
Disable automatic restart on system failure
Disable Driver Signature Enforcement
Disable Early Launch Anti-Malware Driver

Start Windows Normally

Description: View a list of system recovery tools you can use to repair
startup problems, run diagnostics, or restore your system.

ENTER=Choose                                ESC=Cancel
```

Désactiver SAC et le menu de démarrage

Si vous activez SAC et le menu de démarrage, vous pouvez désactiver ces fonctions ultérieurement.

Utilisez l'une des méthodes suivantes pour désactiver SAC et le menu de démarrage sur une instance.

PowerShell

Pour désactiver SAC et le menu de démarrage sur une instance Windows

1. [Connectez-vous](#) à votre instance et effectuez les étapes suivantes à partir d'une ligne de PowerShell commande élevée.
2. Désactivez d'abord le menu de démarrage en changeant la valeur en no.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. Ensuite, désactivez SAC en changeant la valeur en off.

```
bcdedit /ems '{current}' off
```

4. Appliquez la configuration mise à jour en redémarrant l'instance.

```
shutdown -r -t 0
```

Command prompt

Pour désactiver SAC et le menu de démarrage sur une instance Windows

1. [Connectez-vous](#) à votre instance et exécutez les étapes suivantes à partir de l'invite de commandes.
2. Désactivez d'abord le menu de démarrage en changeant la valeur en no.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. Ensuite, désactivez SAC en changeant la valeur en off.

```
bcdedit /ems {current} off
```

4. Appliquez la configuration mise à jour en redémarrant l'instance.

```
shutdown -r -t 0
```

Envoi d'une interruption de diagnostic (utilisateurs avancés uniquement)

Warning

Les interruptions de diagnostic sont destinées à être utilisées par les utilisateurs avancés. Une utilisation incorrecte pourrait avoir un impact négatif sur votre instance. L'envoi d'une interruption de diagnostic à une instance peut déclencher un plantage et un redémarrage d'une instance, ce qui peut entraîner la perte de données.

Vous pouvez envoyer une interruption de diagnostic à une instance inaccessible ou ne répondant pas pour déclencher manuellement une panique au niveau du noyau pour une instance Linux, ou une erreur d'arrêt (communément appelée erreur d'écran bleu) pour une instance Windows.

Instances Linux

Les systèmes d'exploitation Linux tombent généralement en panne et redémarrent en cas de panique de noyau. Le comportement spécifique du système d'exploitation dépend de sa configuration. Vous pouvez aussi utiliser une panique de noyau pour que le noyau système du système d'exploitation de l'instance effectue des tâches telles que la génération d'un fichier de vidage sur incident. Vous pouvez alors utiliser les informations du fichier de vidage sur incident pour effectuer l'analyse de la cause de la panne et le débogage de l'instance. Les données de vidage sur incident sont générées localement par le système d'exploitation sur l'instance elle-même.

instances Windows

En général, les systèmes d'exploitation Windows tombent en panne et redémarrent en cas d'erreur d'arrêt, mais le comportement du système dépend de sa configuration. Une erreur d'arrêt peut également provoquer l'écriture d'informations de débogage dans un fichier par le système d'exploitation (par exemple, vidage mémoire du noyau). Vous pouvez ensuite utiliser ces informations pour effectuer une analyse de la cause racine et déboguer l'instance. Les données de vidage mémoire sont générées localement par le système d'exploitation sur l'instance elle-même.

Avant d'envoyer une interruption de diagnostic à votre instance, nous vous recommandons de consulter la documentation de votre système d'exploitation, puis d'apporter les modifications nécessaires à la configuration.

Sommaire

- [Types d'instance pris en charge](#)
- [Prérequis](#)
- [Envoi d'une interruption de diagnostic](#)

Types d'instance pris en charge

L'interruption diagnostique est prise en charge sur tous les types d'instances basées sur Nitro, à l'exception de celles alimentées par des processeurs AWS Graviton. Pour plus d'informations, consultez [les instances basées sur le système AWS Nitro](#) et [AWS Graviton](#).

Prérequis

Avant d'utiliser une interruption de diagnostic, vous devez configurer le système d'exploitation de votre instance. Cela garantit qu'il exécute les actions dont vous avez besoin en cas de panique du noyau (instances Linux) ou d'erreur d'arrêt (instances Windows).

Instances Linux

Pour configurer Amazon Linux 2 pour générer un vidage sur incident en cas de panique de noyau

1. Connectez-vous à votre instance.
2. Installez kexec et kdump.

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. Configurez le noyau afin qu'il réserve une quantité appropriée de mémoire pour le noyau secondaire. La quantité de mémoire à réserver dépend de la quantité de mémoire totale disponible de votre instance. Ouvrez le fichier `/etc/default/grub` à l'aide de votre éditeur de texte préféré, localisez la ligne commençant par `GRUB_CMDLINE_LINUX_DEFAULT`, puis ajoutez le paramètre `crashkernel` au format suivant : `crashkernel=memory_to_reserve`. Par exemple, pour réserver 160MB, modifiez le fichier `grub` comme suit :

```
GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=160M console=tty0 console=ttyS0,115200n8
net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
rd.shell=0"
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. Enregistrez les modifications, puis fermez le fichier `grub`.

5. Générez à nouveau le fichier de configuration GRUB2.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Sur les instances basées sur les processeurs Intel et AMD, la commande `send-diagnostic-interrupt` envoie une interruption non masquable (NMI) inconnue à l'instance. Vous devez configurer le noyau pour tomber en panne lorsqu'il reçoit l'interruption NMI inconnue. Ouvrez le fichier `/etc/sysctl.conf` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
kernel.unknown_nmi_panic=1
```

7. Redémarrez votre instance et reconnectez-la.
8. Vérifiez que le noyau a été démarré avec le paramètre `crashkernel` correct.

```
$ grep crashkernel /proc/cmdline
```

L'exemple de sortie suivant illustre une configuration réussie.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-  
e38f-408e-878b-fed395b47ad6 ro crashkernel=160M console=tty0 console=ttyS0,115200n8  
net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff  
rd.shell=0
```

9. Vérifiez que le service `kdump` est en cours d'exécution.

```
[ec2-user ~]$ systemctl status kdump.service
```

L'exemple de sortie suivant présente le résultat lorsque le service `kdump` est en cours d'exécution.

```
kdump.service - Crash recovery kernel arming  
  Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:  
  enabled)  
  Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago  
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)  
  Main PID: 2503 (code=exited, status=0/SUCCESS)
```

Note

Par défaut, le fichier de vidage sur incident est enregistré dans `/var/crash/`. Pour modifier cet emplacement, modifiez le fichier `/etc/kdump.conf` à l'aide de l'éditeur de texte de votre choix.

Pour configurer Amazon Linux pour générer un vidage sur incident en cas de panique de noyau

1. Connectez-vous à votre instance.
2. Installez `kexec` et `kdump`.

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. Configurez le noyau afin qu'il réserve une quantité appropriée de mémoire pour le noyau secondaire. La quantité de mémoire à réserver dépend de la quantité de mémoire totale disponible de votre instance.

```
$ sudo grubby --args="crashkernel=memory_to_reserve" --update-kernel=ALL
```

Par exemple, pour réserver 160MB pour le noyau d'incident, utilisez la commande qui suit.

```
$ sudo grubby --args="crashkernel=160M" --update-kernel=ALL
```

4. Sur les instances basées sur les processeurs Intel et AMD, la commande `send-diagnostic-interrupt` envoie une interruption non masquable (NMI) inconnue à l'instance. Vous devez configurer le noyau pour tomber en panne lorsqu'il reçoit l'interruption NMI inconnue. Ouvrez le fichier `/etc/sysctl.conf` à l'aide de l'éditeur de texte de votre choix et ajoutez ce qui suit.

```
kernel.unknown_nmi_panic=1
```

5. Redémarrez votre instance et reconnectez-la.
6. Vérifiez que le noyau a été démarré avec le paramètre `crashkernel` correct.

```
$ grep crashkernel /proc/cmdline
```

L'exemple de sortie suivant illustre une configuration réussie.

```
root=LABEL=/ console=tty1 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295  
LANG=en_US.UTF-8 KEYTABLE=us crashkernel=160M
```

7. Vérifiez que le service kdump est en cours d'exécution.

```
[ec2-user ~]$ sudo service kdump status
```

Si le service est en cours d'exécution, la commande renvoie la réponse `Kdump is operational`.

Note

Par défaut, le fichier de vidage sur incident est enregistré dans `/var/crash/`. Pour modifier cet emplacement, modifiez le fichier `/etc/kdump.conf` à l'aide de l'éditeur de texte de votre choix.

Pour configurer SUSE Linux Enterprise, Ubuntu ou Red Hat Enterprise Linux

Sur les instances basées sur les processeurs Intel et AMD, la commande `send-diagnostic-interrupt` envoie une interruption non masquable (NMI) inconnue à l'instance. Vous devez configurer le noyau pour qu'il se bloque lorsqu'il reçoit le NMI inconnu en ajustant le fichier de configuration de votre système d'exploitation. Pour plus d'informations sur la façon de configurer le noyau pour qu'il plante, consultez la documentation de votre système d'exploitation :

- [SUSE Linux Enterprise](#)
- [Ubuntu](#)
- [Red Hat Enterprise Linux \(RHEL\)](#)

instances Windows

Pour configurer Windows afin qu'il génère un vidage mémoire en d'erreur d'arrêt

1. Connectez-vous à votre instance.
2. Ouvrez le Panneau de configuration, choisissez Système, Paramètres système avancés.
3. Dans la boîte de dialogue Propriétés, choisissez l'onglet Paramètres système avancés.

4. Dans la section Démarrage et récupération, choisissez Paramètres....
5. Dans la section System failure (Échec système), configurez les paramètres comme vous le souhaitez, puis choisissez OK.

Pour plus d'informations sur la configuration des erreurs d'arrêt de Windows, veuillez consulter [Overview of memory dump file options for Windows](#).

Envoi d'une interruption de diagnostic

Une fois que vous avez effectué les modifications de configuration nécessaires, vous pouvez envoyer une interruption de diagnostic à votre instance à l'aide de l'API Amazon EC2 AWS CLI ou Amazon EC2.

AWS CLI

Pour envoyer une interruption de diagnostic à votre instance (AWS CLI)

Utilisez la commande [send-diagnostic-interrupt](#) et spécifiez l'ID de l'instance.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

Pour envoyer une interruption de diagnostic à votre instance (AWS Tools for Windows PowerShell)

Utilisez le [Send-EC2DiagnosticInterrupt](#)cmdlet et spécifiez l'ID de l'instance.

```
PS C:\> Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Historique du document

Le tableau suivant décrit les ajouts importants au guide de l'utilisateur Amazon EC2 à compter de 2019. Nous mettons également fréquemment à jour le guide pour répondre aux commentaires que vous nous envoyez.

Modification	Description	Date
outil de recherche de type d'instance EC2 : paramètres supplémentaires	L'outil de recherche de type d'instance EC2 fournit désormais des paramètres supplémentaires vous permettant de définir des exigences plus détaillées pour votre charge de travail.	5 juin 2024
Instances U7i-12TB, U7in-16TB, U7in-24TB et U7in-32TB	Nouveaux types d'instances à mémoire élevée dotés de processeurs Intel Xeon Scalable de 4e génération.	28 mai 2024
Nouvelle politique gérée pour EC2 Fast Launch	Ajout de la EC2FastLaunchFullAccess politique permettant d'effectuer des actions d'API liées à la fonctionnalité EC2 Fast Launch à partir d'une instance.	14 mai 2024
Protection contre le désenregistrement de l'AMI	Vous pouvez activer la protection de désenregistrement sur une AMI pour empêcher toute suppression accidentelle ou malveillante.	23 avril 2024
Horloge matérielle PTP — prise en charge des types d'instance	L'horloge matérielle PTP est désormais disponible sur les	22 avril 2024

	types d'instances C7a, C7i, M7a, M7g, M7i, R7a et R7i.	
Ajout de considérations relatives aux performances de Nitro pour une mise en réseau améliorée	Cette page se concentre sur les considérations relatives au réseau afin de vous aider à optimiser les performances de vos instances Amazon EC2 basées sur Nitro.	4 avril 2024
Nouvelle politique gérée pour les instantanés EBS compatibles VSS	Amazon EC2 VSS propose une nouvelle politique gérée par IAM que vous pouvez ajouter à votre rôle de profil d'instance pour garantir le maintien de vos autorisations up-to-date et respecter les meilleures pratiques.	28 mars 2024
Horloge matérielle PTP — USA Est (Virginie du Nord)	L'horloge matérielle PTP est désormais disponible dans la région USA Est (Virginie du Nord).	26 mars 2024
Définir IMDSv2 comme compte par défaut	Vous pouvez configurer tous les nouveaux lancements d'instances EC2 dans votre compte pour utiliser le service de métadonnées d'instance version 2 (IMDSv2) par défaut.	25 mars 2024
Marquer les nouvelles AMI Linux créées à partir d'un instantané	Lorsque vous créez une AMI Linux à partir d'un instantané, vous pouvez baliser la nouvelle AMI.	7 mars 2024

[Marquez les nouvelles AMI et les nouveaux instantanés lors de la copie](#)

Lorsque vous copiez une AMI, vous pouvez étiqueter la nouvelle AMI et les nouveaux instantanés avec les mêmes balises, ou vous pouvez les étiqueter avec des balises différentes.

7 mars 2024

[Supprimer les pages AWS du pack d'administration](#)

Le pack d' AWS administration était principalement utilisé avec Windows Server 2012 et versions antérieures. Ces anciennes versions de plate-forme de système d'exploitation ne sont plus prises en charge. Pour gérer et dépanner votre parc de serveurs fonctionnant sur site AWS et sur site, consultez [AWS Systems Manager Fleet Manager](#).

12 février 2024

[EC2 Instance Connect préinstallé sur les AMI macOS](#)

EC2 Instance Connect est désormais préinstallé sur les AMI macOS Sonoma 14.2.1 ou version ultérieure, macOS Ventura 13.6.3 ou version ultérieure et macOS Monterey 12.7.2 ou version ultérieure.

26 janvier 2024

[Prise en charge d'EC2 Instance Connect pour CentOS, macOS et RHEL](#)

Vous pouvez désormais installer EC2 Instance Connect sur les AMI CentOS, macOS et RHEL prises en charge.

6 décembre 2023

[Prise en charge de la mise en veille prolongée pour C7a, C7i, R7a, R7i et R7iz](#)

Désormais, vous pouvez mettre en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instances C7a, C7i, R7a, R7i et R7iz.

1er décembre 2023

[Sélecteur de type d'instance Amazon Q EC2](#)

Le sélecteur de type d'instance Amazon Q EC2 prend en compte votre cas d'utilisation, votre type de charge de travail et les préférences du fabricant du processeur, ainsi que la façon dont vous priorisez le prix et les performances. Il utilise ensuite ces données pour fournir des conseils et des suggestions concernant les types d'instances Amazon EC2 les mieux adaptés à vos nouvelles charges de travail.

28 novembre 2023

[Offre gratuite EC2](#)

Vous pouvez suivre votre utilisation de l'offre gratuite EC2 à partir du tableau de bord EC2.

26 novembre 2023

[Console-to-Code](#)

Console-to-Code peut vous aider à faire vos premiers pas avec le code d'automatisation. Console-to-Code enregistre les actions de votre console, puis utilise l'IA générative pour suggérer du code dans votre infrastructure préférée au format de code. Vous pouvez utiliser le code comme point de départ, en le personnalisant pour qu'il soit prêt pour la production en fonction de votre cas d'utilisation spécifique.

26 novembre 2023

[Délais de suivi d'inactivité de connexion configurables](#)

Les connexions de groupe de sécurité qui restent inactives peuvent entraîner l'épuisement du suivi des connexions, empêcher le suivi des connexions et entraîner la perte de paquets. Vous pouvez désormais définir le délai en secondes pour le suivi de connexion de groupe de sécurité sur une interface réseau Elastic.

17 novembre 2023

[Horloge matérielle PTP](#)

Les instances prises en charge disposent désormais d'une horloge matérielle PTP (Precision Time Protocol). L'horloge matérielle PTP prend en charge le protocole NTP ou une connexion PTP directe.

16 novembre 2023

Modification du type d'instance d'une instance dont la mise en veille prolongée est activée	Vous pouvez désormais modifier le type d'une instance dont la mise en veille prolongée est activée lorsqu'il est à l'état stopped.	16 novembre 2023
Topologie d'instance	Vous pouvez utiliser l' DescribeInstanceTopology API pour détecter l'emplacement de vos instances, puis utiliser ces informations pour optimiser les tâches HPC et ML en les exécutant sur des instances physiquement plus proches les unes des autres.	13 novembre 2023
Support des AMI partagées EC2 Fast Launch	Vous pouvez désormais activer EC2 Fast Launch sur une AMI partagée avec vous. Lorsque vous activez EC2 Fast Launch sur une AMI partagée, les instantanés préconfigurés pour un lancement plus rapide sont créés dans votre compte.	6 novembre 2023
Blocs de capacité pour ML	Vous pouvez désormais réserver des instances GPU à une date ultérieure pour prendre en charge vos charges de travail de machine learning (ML) de courte durée.	31 octobre 2023

Mise en veille prolongée d'instances Spot	Vous pouvez désormais mettre en veille prolongée vos instances Spot en utilisant la même expérience de mise en veille prolongée et les mêmes familles d'instances que celles actuellement disponibles pour les instances à la demande.	24 octobre 2023
Paramètres par défaut pour bloquer l'accès public aux AMI	Les paramètres pour bloquer l'accès public aux AMI sont désormais activés par défaut pour tous les nouveaux comptes et pour les comptes existants sans AMI publiques.	20 octobre 2023
Amazon EC2 Global View (Amazon EC2 Global View)	Amazon EC2 Global View prend en charge des types de ressources supplémentaires et des options d'affichage personnalisables.	18 octobre 2023
Prise en charge de la mise en veille prolongée pour Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Mettez en veille prolongée vos instances récemment lancées à partir de l'AMI Ubuntu 22.04.2 LTS (Jammy Jellyfish).	16 octobre 2023
Désactiver une AMI	Vous pouvez désactiver une AMI pour empêcher son utilisation pour le lancement d'instances.	12 octobre 2023

Contrôles de statut de l'EBS attachés	Vous pouvez utiliser les contrôles de statut de l'EBS attaché pour surveiller si les volumes Amazon EBS attachés à une instance sont accessibles.	11 octobre 2023
Prise en charge de la mise en veille prolongée pour Red Hat Enterprise Linux 9	Mettez en veille prolongée vos instances récemment lancées à partir de l'AMI Red Hat Enterprise Linux 9.	2 octobre 2023
Prise en charge de la mise en veille prolongée pour Microsoft Windows Server 2022	Mettez en veille prolongée vos instances récemment lancées à partir de l'AMI Microsoft Windows Server 2022.	2 octobre 2023
Prise en charge de la mise en veille prolongée pour AL2023	Mettez en veille prolongée vos instances récemment lancées à partir de l'AMI AL2023.	2 octobre 2023
Lancer l'interruption des instances Spot dans un parc d'instances Spot	Vous pouvez sélectionner un parc d'instances Spot dans la console Amazon EC2 et lancer une interruption d'instances Spot dans la flotte afin de tester la façon dont les applications de vos instances Spot gèrent les interruptions.	21 septembre 2023
Bloquer l'accès public pour les AMI	Vous pouvez activer le blocage de l'accès public pour les AMI au niveau du compte afin de bloquer toute tentative de rendre vos AMI publiques.	12 septembre 2023

Prise en charge de la mise en veille prolongée pour M7i et M7i-flex	Désormais, vous pouvez mettre en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instances M7i et M7i-flex	22 août 2023
EC2-Classic est obsolète.	Avec EC2-Classic, les instances EC2 s'exécutent dans un réseau plat unique partagé avec d'autres clients. Amazon VPC remplace EC2-Classic. Avec Amazon VPC, vos instances s'exécutent dans un cloud privé virtuel (VPC) qui est logiquement isolé sur votre compte AWS .	08/08/2023
Hôtes dédiés	Vous pouvez allouer des hôtes dédiés sur des actifs matériels spécifiques sur un Outpost.	20 juin 2023
Point de terminaison EC2 Instance Connect	Vous pouvez désormais vous connecter à une instance via SSH ou RDP sans qu'il soit nécessaire que l'instance ait une adresse IPv4 publique.	13 juin 2023
Analyseur de packages IMDS	Vous pouvez désormais utiliser l'analyseur de packages IMDS pour identifier les sources des appels IMDSv1 sur vos instances EC2.	1er juin 2023

Instances de matériel nu EC2 Serial Console	EC2 Serial Console prend désormais en charge la connectivité au port série des instances de matériel nu sélectionnées.	11 avril 2023
Quotas de modèles de lancement	Vous pouvez désormais consulter vos quotas pour les modèles de lancement et leurs versions dans la console Service Quotas et à l'aide de la CLI Service Quotas.	3 avril 2023
Notifications d'utilisation des réserves de capacité	AWS Health envoie désormais des notifications lorsque le taux d'utilisation des capacités pour les réservations de capacité de votre compte tombe en dessous de 20 %.	3 avril 2023
Groupes de réserve de capacité	Vous pouvez désormais ajouter des réserves de capacité qui sont partagées avec vous aux groupes de réserves de capacité qui vous appartiennent.	30 mars 2023
Modifier les options des métadonnées d'instance	Vous pouvez désormais utiliser la console Amazon EC2 pour modifier les options des métadonnées d'instance.	20 mars 2023

Mises à jour du système d'exploitation macOS sur place	Vous pouvez désormais effectuer des mises à jour sur place du système d'exploitation macOS d'Apple sur les instances Mac M1.	14 mars 2023
UEFI préférée	Vous pouvez désormais créer une AMI unique qui prend en charge à la fois l'interface UEFI (Unified Extensible Firmware Interface) et les modes de démarrage du BIOS hérité.	3 mars 2023
Modifier une AMI pour IMDSv2	Modifiez votre AMI existante de telle sorte que les instances lancées à partir de l'AMI nécessitent IMDSv2 par défaut.	28 février 2023
Sécurité basée sur la virtualisation de Windows – Credential Guard	Vous pouvez activer Credential Guard, une fonction de sécurité basée sur la virtualisation (VBS), sur les instances Amazon EC2 prises en charge.	31 janvier 2023
Alias AMI dans les modèles de lancement	Vous pouvez spécifier un AWS Systems Manager paramètre au lieu de l'ID d'AMI dans vos modèles de lancement afin d'éviter de devoir mettre à jour les modèles chaque fois que l'ID d'AMI change.	19 janvier 2023

[Prise en charge de la mise en veille prolongée pour C6i, i3en et M6i](#)

Désormais, vous pouvez mettre en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instances C6i, I3en et M6i.

19 décembre 2022

[Prévention des écritures déchirées](#)

Améliorez les performances de vos charges de travail de bases de données relationnelles gourmandes en E/S et réduisez la latence sans affecter négativement la résilience des données grâce à la fonction de prévention des écritures déchirées, une fonctionnalité de stockage par blocs.

29 novembre 2022

[ENA Express](#)

Augmentez le débit et minimisez la latence de queue du trafic réseau entre les instances EC2 avec ENA Express.

28 novembre 2022

[Verrouillage d'une règle de conservation de la corbeille](#)

Vous pouvez verrouiller vos règles de conservation pour les protéger contre les modifications et les suppressions accidentelles ou malveillantes.

23 novembre 2022

[Copier les balises d'AMI](#)

Lorsque vous copiez une AMI, vous pouvez copier simultanément vos balises d'AMI définies par l'utilisateur.

18 novembre 2022

[Taille de l'AMI pour le stockage et la restauration](#)

La taille d'une AMI (avant compression) pouvant être stockée et restaurée depuis et vers un compartiment Amazon S3 peut désormais atteindre 5 000 Go.

16 novembre 2022

[priceCapacityOptimizedstratégie d'allocation pour les instances Spot](#)

Un parc d'instances Spot qui utilise la stratégie d'allocation `priceCapacityOptimized` examine à la fois le prix et la capacité pour sélectionner les groupes d'instances Spot les moins susceptibles d'être interrompus et dont le prix est le plus bas possible.

10 novembre 2022

[price-capacity-optimizedstratégie d'allocation pour les instances Spot](#)

Une flotte EC2 qui utilise la stratégie d'allocation `price-capacity-optimized` examine à la fois le prix et la capacité pour sélectionner les groupes d'instances Spot les moins susceptibles d'être interrompus et dont le prix est le plus bas possible.

10 novembre 2022

[Annulation du partage d'une AMI avec votre compte](#)

Si une AMI a été partagée avec votre Compte AWS et que vous ne souhaitez plus qu'elle soit partagée avec votre compte, vous pouvez supprimer votre compte des autorisations de lancement de l'AMI.

4 novembre 2022

Transfert d'adresses IP Elastic	Vous pouvez désormais transférer des adresses IP élastiques de l'une Compte AWS à l'autre.	31 octobre 2022
Remplacement d'un volume racine	Vous pouvez remplacer le volume Amazon EBS racine pour une instance en cours d'exécution à l'aide d'une AMI.	27 octobre 2022
Connexion automatique d'une instance à une base de données	Utilisez la fonction de connexion automatique pour connecter rapidement une ou plusieurs instances EC2 à une base de données RDS afin de permettre le trafic entre elles.	10 octobre 2022
Quotas d'AMI	Les quotas s'appliquent désormais à la création et au partage des AMI.	10 octobre 2022
Configurer une AMI pour IMDSv2	Configurez votre AMI de telle sorte que les instances lancées à partir de l'AMI nécessitent IMDSv2 par défaut.	3 octobre 2022
Lancer une interruption d'instance Spot	Vous pouvez sélectionner une instance Spot dans la console Amazon EC2 et lancer une interruption afin de tester la façon dont les applications de vos instances Spot gèrent les interruptions.	26 septembre 2022

Fournisseur d'AMI vérifié	Dans la console Amazon EC2, les AMI publiques détenues par Amazon ou par un partenaire Amazon vérifié sont certifiées Fournisseur vérifié.	22 juillet 2022
Groupes de placement sur AWS Outposts	Ajout d'une stratégie de répartition des hôtes pour les groupes de placement sur un Outpost.	30 juin 2022
Clés de condition pour la corbeille	Vous pouvez utiliser les clés de condition <code>rbin:Request/ResourceType</code> et <code>rbin:Attribute/ResourceType</code> pour filtrer l'accès sur les demandes de corbeille.	14 juin 2022
Volumes io2 Block Express	Vous pouvez modifier la taille et les IOPS provisionnés des volumes io2 Block Express et vous pouvez les activer pour une restauration rapide des instantanés.	31 mai 2022
Hôtes dédiés sur AWS Outposts	Vous pouvez allouer des hôtes dédiés sur AWS Outposts.	31 mai 2022
Protection contre l'arrêt d'instance	Pour éviter que votre instance ne soit arrêtée accidentellement, vous pouvez activer la protection contre l'arrêt de l'instance.	24 mai 2022

UEFI Secure Boot	UEFI Secure Boot s'appuie sur le processus de démarrage sécurisé de longue date d'Amazon EC2 et fournit des fonctionnalités defense-in-depth supplémentaires qui aident les clients à protéger leurs logiciels contre les menaces persistantes après les redémarrages.	10 mai 2022
NitroTPM	Le module Nitro Trusted Platform (NitroTPM) est un appareil virtuel fourni par le système AWS Nitro et conforme à la spécification TPM 2.0.	10 mai 2022
Événements de changement d'état de l'AMI	Amazon EC2 génère désormais un événement lorsqu'une AMI change d'état. Vous pouvez utiliser Amazon EventBridge pour détecter ces événements et y réagir.	9 mai 2022
Décrire les clés publiques	Vous pouvez interroger la clé publique et la date de création d'une paire de clés Amazon EC2.	28 avril 2022
Création des paires de clés	Vous pouvez spécifier le format de clé (PEM ou PPK) lors de la création d'une nouvelle paire de clés.	28 avril 2022

Monter les systèmes de fichiers Amazon FSx au lancement	Vous pouvez monter un système de fichiers Amazon FSx pour NetApp ONTAP ou Amazon FSx pour OpenZFS nouveau ou existant au lancement à l'aide du nouvel assistant de lancement d'instance.	12 avril 2022
Nouvel assistant de lancement d'instance	Une nouvelle expérience de lancement améliorée dans la console Amazon EC2, pour lancer les instances EC2 plus rapidement et plus facilement.	5 avril 2022
Obsolescence automatique des AMI publiques	Par défaut, la date d'obsolescence de toutes les AMI publiques est fixée à deux ans à compter de la date de création de l'AMI.	31 mars 2022
Catégorie de métadonnées d'instance : autoscaling/target-lifecycle-state	Lorsque vous utilisez des groupes Auto Scaling, vous pouvez accéder à l'état du cycle de vie cible d'une instance à partir des métadonnées de l'instance.	24 mars 2022
Dernière heure de lancement de l'AMI	Le <code>lastLaunchedTime</code> indique quand votre AMI a été utilisée pour la dernière fois pour lancer une instance.	28 février 2022
Corbeille pour AMI	La corbeille vous permet de restaurer les AMI supprimées accidentellement.	3 février 2022

Clés ED25519	Les clés ED25519 sont maintenant prises en charge pour les instances EC2 Connect et EC2 Serial Console.	20 janvier 2022
Plateformes RHEL supplémentaires pour les réserves de capacité	Plateformes Red Hat Enterprise Linux supplémentaires pour les réserves de capacité à la demande.	11 janvier 2022
Configurer les AMI Windows pour un lancement plus rapide	Configurez les AMI Windows pour lancer des instances jusqu'à 65 % plus rapidement à l'aide d'instancés approuvés préalablement.	10 janvier 2022
Identifications d'instance dans les métadonnées d'instance	Vous pouvez accéder aux identifications d'une instance à partir des métadonnées de l'instance.	6 janvier 2022
Réserves de capacité dans des groupes de placement de cluster	Vous pouvez créer des réserves de capacité dans des groupes de placement de cluster.	6 janvier 2022
Corbeille pour instantanés Amazon EBS	La corbeille des instantanés Amazon EBS est une fonction de récupération d'instancés qui vous permet de restaurer des instantanés supprimés accidentellement.	29 novembre 2021

Parc d'instances Spot launch-before-terminate	Un parc d'instances Spot peut mettre fin aux instances Spot qui reçoivent une notification de rééquilibrage après le lancement de nouvelles instances Spot de remplacement.	4 novembre 2021
EC2 Fleet launch-before-terminate	Une flotte EC2 peut mettre fin aux instances Spot qui reçoivent une notification de rééquilibrage après le lancement de nouvelles instances Spot de remplacement.	4 novembre 2021
Comparer les horodatages	Vous pouvez déterminer l'heure réelle d'un événement en comparant l'horodatage de votre instance Linux Amazon EC2 avec. ClockBound	2 novembre 2021
Partager des AMI avec des organisations et des unités d'organisations	Vous pouvez désormais partager des AMI avec les AWS ressources suivantes : organisations et unités organisationnelles (UO).	29 octobre 2021
Score de placement Spot	Obtenez une recommandation pour une AWS région ou une zone de disponibilité en fonction de vos besoins en matière de capacité Spot.	27 octobre 2021

Sélection de type d'instance basée sur des attributs pour un parc d'instances Spot	Spécifiez les attributs qu'une instance doit posséder, et Amazon EC2 identifiera tous les types d'instance avec ces attributs.	27 octobre 2021
Sélection de type d'instance basée sur des attributs pour la flotte EC	Spécifiez les attributs qu'une instance doit posséder, et Amazon EC2 identifiera tous les types d'instance avec ces attributs.	27 octobre 2021
Flotte de réservation de capacité à la demande	Vous pouvez utiliser une flotte de réservations de capacité pour lancer un groupe, ou une flotte, de réservations de capacité.	5 octobre 2021
Prise en charge de la mise en veille prolongée pour Ubuntu 20.04 LTS - Focal	Mettez en veille prolongée vos instances récemment lancées à partir de l'AMI Ubuntu 20.04 LTS - Focal.	4 octobre 2021
Flotte EC2 et réservations de capacité à la demande	La flotte EC2 peut lancer les instances à la demande dans réservations de capacité targeted.	22 septembre 2021
instances T3 sur les hôtes dédiés	Prise en charge des instances T3 sur l'hôte dédié Amazon EC2	14 septembre 2021
Prise en charge de la mise en veille prolongée pour RHEL, Fedora et CentOS	Mettez en veille vos instances nouvellement lancées à partir des AMI RHEL, Fedora et CentOS.	9 septembre 2021

Amazon EC2 Global View (Amazon EC2 Global View)	Amazon EC2 Global View vous permet de visualiser les VPC, les sous-réseaux, les instances, les groupes de sécurité et les volumes dans plusieurs AWS régions sur une seule console.	1er septembre 2021
Prise en charge de l'obsolescence des AMI pour Amazon Data Lifecycle Manager	Les politiques d'AMI EBS Amazon Data Lifecycle Manager peuvent rendre obsolètes les AMI. La politique AWSDataLifecycleManagerServiceRoleForAMIManagement AWS gérée a été mise à jour pour prendre en charge cette fonctionnalité.	23 août 2021
Prise en charge de la mise en veille prolongée pour C5d, M5d et R5d	Vous pouvez mettre en veille prolongée les instances nouvellement lancées et qui s'exécutent sur les types d'instances C5d, M5d et R5d.	19 août 2021
Paires de clés Amazon EC2	Amazon EC2 prend désormais en charge les clés ED25519 sur les instances Linux et Mac.	17 août 2021
Préfixes pour les interfaces réseau	Vous pouvez attribuer une plage CIDR IPv4 ou IPv6 privée, automatiquement ou manuellement, à vos interfaces réseau.	22 juillet 2021

Fenêtres d'événements	Vous pouvez définir des fenêtres d'événements hebdomadaires personnalisées récurrentes pour des événements planifiés qui redémarrent, arrêtent ou résilient vos instances Amazon EC2.	15 juillet 2021
ID de ressource et prise en charge de l'identification pour les règles de groupes de sécurité	Vous pouvez faire référence aux règles des groupes de sécurité par ID de ressource . Vous pouvez également ajouter des étiquettes aux règles de vos groupes de sécurité.	7 juillet 2021
Rendre obsolète une AMI	Vous pouvez maintenant spécifier quand une AMI est obsolète.	11 juin 2021
Facturation à la seconde Windows	Amazon EC2 facture l'utilisation de Windows et de SQL Server à la seconde, avec un minimum d'une minute.	10 juin 2021
Réservations de capacité sur AWS Outposts	Vous pouvez désormais utiliser les réservations de capacité sur AWS Outposts.	24 mai 2021
Partage d'une Réserve de capacité	Les réservations de capacité créés dans Local Zones et zones Wavelength peuvent maintenant être partagés.	24 mai 2021

Remplacement du volume racine	Vous pouvez désormais utiliser les tâches de remplacement du volume racine pour remplacer le volume EBS racine des instances en cours d'exécution.	22 avril 2021
Stocker et restaurer une AMI à l'aide de S3	Stockez les AMI basées sur EBS dans S3 et restaurez-les à partir de S3 pour permettre la copie des AMI entre partitions.	6 avril 2021
EC2 Serial Console	Résolvez les problèmes de démarrage et de connectivité réseau en établissant une connexion au port série d'une instance.	30 mars 2021
Modes de démarrage	Amazon EC2 prend désormais en charge le démarrage UEFI sur certaines instances EC2 AMD et Intel.	22 mars 2021
Créer un enregistrement DNS inverse	Vous pouvez désormais configurer la recherche DNS inverse pour vos adresses IP Elastic.	3 février 2021
Étiqueter les AMI et les instantanés lors de la création des AMI	Lorsque vous créez une AMI, vous pouvez baliser celle-ci et les instantanés en utilisant les mêmes balises ou à l'aide de balises différentes.	4 décembre 2020

Utilisez Amazon EventBridge pour surveiller les événements de Spot Fleet	Créez des EventBridge règles qui déclenchent des actions programmatiques en réponse aux changements d'état et aux erreurs de Spot Fleet.	20 novembre 2020
Utilisez Amazon EventBridge pour surveiller les événements de la flotte EC2	Créez des EventBridge règles qui déclenchent des actions programmatiques en réponse aux changements et aux erreurs de l'état de la flotte EC2.	20 novembre 2020
Supprimer instant les flottes	Supprimez une flotte EC2 de type <code>instant</code> et mettez hors service toutes les instances de la flotte avec un seul appel d'API.	18 novembre 2020
Prise en charge de la mise en veille prolongée pour T3 et T3a	Mettez en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instance T3 et T3a.	17 novembre 2020
Amazon EFS Quick Create	Vous pouvez créer et monter un système de fichiers Amazon EFS sur une instance au lancement à l'aide d'Amazon EFS Quick Create.	9 novembre 2020
Catégorie de métadonnées d'instance : <code>events/recommendations/rebalance</code>	Heure approximative, UTC, à laquelle la notification de recommandation de rééquilibrage d'instance EC2 est émise pour l'instance.	4 novembre 2020
Recommandation de rééquilibrage des instances EC2	Signal qui vous avertit en cas de risque élevé d'interruption d'instance Spot.	4 novembre 2020

Réervations de capacité dans les zones Wavelength	Les réservations de capacité peuvent maintenant être créées et utilisées dans les zones Wavelength.	4 novembre 2020
Rééquilibrage de la capacité	Configurez le parc d'instances Spot ou la flotte EC2 pour lancer une instance Spot de remplacement lorsqu'Amazon EC2 émet une recommandation de rééquilibrage.	4 novembre 2020
Prise en charge de la mise en veille prolongée pour les types d'instance I3, M5ad et R5ad	Mettez en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instances I3, M5ad et R5ad.	21 octobre 2020
Limites du vCPU d'instance Spot	Les limites d'instance Spot sont maintenant gérées en fonction du nombre de vCPU que vos instances Spot en cours d'exécution utilisent ou utiliseront en attendant le traitement des demandes ouvertes.	1er octobre 2020
Réervations de capacité dans Local Zones	Réservations de capacité peut maintenant être créé et utilisé dans Local Zones.	30 septembre 2020
Prise en charge de la mise en veille prolongée pour M5a et R5a	Désormais, vous pouvez mettre en veille prolongée les instances que vous venez de lancer et qui s'exécutent sur les types d'instances M5a et 5Ra.	28 août 2020

[Les métadonnées d'instance fournissent des informations sur l'emplacement et le placement](#)

Nouveaux champs de métadonnées d'instance dans la catégorie placement : région, nom du groupe de placement, numéro de partition, ID d'hôte et ID de zone de disponibilité.

24 août 2020

[Groupes de réserve de capacité](#)

Vous pouvez utiliser AWS Resource Groups pour créer des collections logiques de réservations de capacité, puis lancer des instances cibles dans ces groupes.

29 juillet 2020

[EC2Launch v2](#)

Vous pouvez utiliser EC2Launch v2 pour effectuer des tâches pendant le démarrage de l'instance, si une instance est arrêtée et démarrée ultérieurement, si une instance est redémarrée et à la demande. EC2Launch v2 prend en charge toutes les versions de Windows Server et remplace EC2Launch et EC2Config.

30 juin 2020

[Apportez vos propres adresses IPv6](#)

Vous pouvez transférer une partie ou la totalité de votre plage d'adresses IPv6 de votre réseau local vers votre AWS compte.

21 mai 2020

Lancement des instances à l'aide d'un paramètre Systems Manager	Vous pouvez spécifier un AWS Systems Manager paramètre au lieu d'une AMI lorsque vous lancez une instance.	5 mai 2020
Personnaliser les notifications d'événements planifiés	Vous pouvez personnaliser les notifications d'événements planifiés pour inclure des balises dans la notification par e-mail.	4 mai 2020
Amazon Linux 2 Kernel Live Patching	Kernel Live Patching pour Amazon Linux 2 vous permet d'appliquer des correctifs de vulnérabilité de sécurité et de bogues critiques à un noyau Linux en cours d'exécution, sans redémarrer ni interrompre les applications en cours d'exécution.	28 avril 2020
Windows Server sur les hôtes dédiés	Vous pouvez utiliser les AMI Windows Server fournies par Amazon pour exécuter les dernières versions de Windows Server sur des Hôtes dédiés.	7 avril 2020
Arrêter et démarrer une instance Spot	Arrêtez vos instances Spot basées sur Amazon EBS et démarrez-les à votre gré, au lieu de vous fier au comportement d'arrêt sur interruption.	13 janvier 2020

[Étiquette des ressources](#)

Vous pouvez baliser des passerelles Internet de sortie uniquement, des passerelles locales, des tables de routage de passerelle locale, des interfaces virtuelles de passerelle locale, des groupes d'interfaces virtuelles de passerelle locale, des associations de VPC de table de routage de passerelle locale et des associations de groupes d'interface virtuelle de table de routage de passerelle locale.

10 janvier 2020

[Connexion à votre instance à l'aide du Gestionnaire de session](#)

Vous pouvez démarrer une session Session Manager avec une instance à partir de la console Amazon EC2.

18 décembre 2019

[Hôtes dédiés et groupes de ressources hôte](#)

Les Hôtes dédiés peuvent désormais être utilisés avec des groupes de ressources hôte.

2 décembre 2019

[Partage d'hôte dédié](#)

Vous pouvez désormais partager vos hôtes dédiés entre plusieurs AWS comptes.

2 décembre 2019

[Spécification de crédits par défaut au niveau du compte](#)

Vous pouvez définir la spécification de crédit par défaut par famille d'instances de performance burstable au niveau du compte par AWS région.

25 novembre 2019

Découverte du type d'instance	Vous pouvez identifier un type d'instance qui répond à vos besoins.	22 novembre 2019
Hôtes dédiés	Vous pouvez désormais configurer un Hôte dédié pour prendre en charge plusieurs types d'instances au sein d'une famille d'instances.	21 novembre 2019
Instance Metadata Service Version 2	Vous pouvez utiliser Service des métadonnées d'instance Version 2, qui est une méthode orientée session de demande de métadonnées d'instance.	19 novembre 2019
Elastic Fabric Adapter (EFA)	Les adaptateurs Elastic Fabric Adapter peuvent désormais être utilisés avec Intel MPI 2019 Update 6.	15 novembre 2019
Prise en charge de la mise en veille pour les instances Windows à la demande	Vous pouvez mettre en veille les instances Windows à la demande	14 octobre 2019
Achats d'instances réservées mis en file d'attente	Vous pouvez mettre l'achat d'une Instance réservée en file d'attente jusqu'à trois ans en avance.	4 octobre 2019
Interruption de diagnostic	Vous pouvez envoyer une interruption de diagnostic à une instance inaccessible ou qui ne répond pas afin de déclencher une panique de noyau.	14 août 2019

Stratégie d'allocation optimisée pour la capacité	À l'aide de la flotte EC2 ou du parc d'instances Spot, vous pouvez lancer des flottes d'instances Spot depuis des groupes Spot avec une capacité optimale pour le nombre d'instances que vous lancez.	12 août 2019
Partage de réserve de capacité à la demande	Vous pouvez désormais partager vos réservations de capacité entre différents AWS comptes.	29 juillet 2019
Elastic Fabric Adapter (EFA)	EFA prend désormais en charge MPI 3.1.4 et Intel MPI 2019 Update 4.	26 juillet 2019
EC2 Instance Connect	EC2 Instance Connect est une solution simple et sécurisée pour vous connecter à vos instances à l'aide de Secure Shell (SSH).	27 juin 2019
Restauration de l'hôte	Redémarre automatiquement vos instances sur un nouvel hôte en cas de panne matérielle soudaine sur un Hôte dédié.	5 juin 2019
Instantanés cohérents par rapport à l'application VSS	Prenez des instantanés cohérents avec les applications de tous les volumes Amazon EBS attachés à vos instances Windows à l'aide de Run Command. AWS Systems Manager	13 mai 2019

[Assistant de recréation de plateformes Windows vers Linux pour les bases de données Microsoft SQL Server](#)

Déplacez les charges de travail Microsoft SQL Server d'un système d'exploitation Windows vers un système d'exploitation Linux.

8 mai 2019

[Mise à niveau automatisée de Windows](#)

Effectuez des mises à niveau automatisées des instances Windows EC2 à l'aide AWS Systems Manager de.

6 mai 2019

[Elastic Fabric Adapter \(EFA\)](#)

Vous pouvez attacher un Elastic Fabric Adapter à vos instances pour accélérer les applications HPC (Calcul Haute Performance).

29 avril 2019

Pour plus d'informations sur les versions des types d'instance pour Amazon EC2, consultez [l'historique des documents](#) dans le guide des types d'instances Amazon EC2.

Historique pour 2018 et les années antérieures

Le tableau suivant décrit les ajouts importants apportés au guide de l'utilisateur Amazon EC2 en 2018 et les années précédentes.

Fonctionnalité	Version de l'API	Description	Date de publication
Groupes de placement par partition	2016-11-15	Les groupes de placement par partition répartissent les instances entre les partitions logiques, en s'assurant que les instances d'une partition ne partagent pas le matériel sous-jacent avec les instances d'autres partitions. Pour plus d'informations, consultez Groupes de placement par partition .	20 décembre 2018

Fonctionnalité	Version de l'API	Description	Date de publication
Mise en veille d'instances EC2 Linux	2016-11-15	Vous pouvez mettre en veille une instance Linux si cette dernière a été activée pour la mise en veille et répond aux exigences de la mise en veille. Pour plus d'informations, consultez Hibernez votre instance Amazon EC2 .	28 novembre 2018
Accélérateurs Amazon Elastic Inference	2016-11-15	Vous pouvez attacher un accélérateur Amazon EI à vos instances pour ajouter une accélération alimentée par GPU afin de réduire le coût d'inférence de deep learning.	28 novembre 2018
Parc d'instances recommandé par la console Spot	2016-11-15	La console Spot recommande une flotte d'instances basé sur les bonnes pratiques Spot (diversification des instances) pour répondre aux spécifications matérielles minimales (vCPU, mémoire et stockage) de vos besoins applicatifs. Pour plus d'informations, consultez Créer une Spot Fleet request .	20 novembre 2018
Nouveau type de demande de flotte EC2 : instant	2016-11-15	La flotte EC2 prend désormais en charge un nouveau type de demande, instant, que vous pouvez utiliser pour allouer de manière synchrone une capacité sur des types d'instance et des modèles d'achat. La demande instant renvoie les instances lancées dans la réponse d'API, sans aucune action supplémentaire. Cela vous permet de contrôler si et quand les instances sont lancées. Pour plus d'informations, consultez Types de demande flotte EC2 .	14 novembre 2018

Fonctionnalité	Version de l'API	Description	Date de publication
Informations d'économies Spot	2016-11-15	Vous pouvez afficher les économies réalisées grâce à l'utilisation d'instances Spot pour un seul parc d'instances Spot ou pour toutes les instances Spot. Pour plus d'informations, consultez Économies réalisées grâce à l'achat d'instances Spot .	5 novembre 2018
Prise en charge de la console pour l'optimisation des options d'UC	2016-11-15	Lorsque vous lancez une instance, vous pouvez optimiser les options d'UC pour répondre à des besoins métier ou des charges de travail spécifiques à l'aide de la console Amazon EC2. Pour plus d'informations, consultez Optimiser les options d'UC .	31 octobre 2018
Prise en charge de la console pour la création d'un modèle de lancement à partir d'une instance	2016-11-15	Vous pouvez créer un modèle de lancement en utilisant une instance comme base d'un nouveau modèle de lancement à l'aide de la console Amazon EC2. Pour plus d'informations, consultez Création d'un modèle de lancement .	30 octobre 2018
On-Demand Capacity Reservations	2016-11-15	Vous pouvez réserver de la capacité pour vos instances Amazon EC2 dans une zone de disponibilité spécifique pour la durée de votre choix. Cela vous permet de créer et de gérer des réservations de capacité indépendamment des remises de facturation offertes par les instances réservées (IR). Pour plus d'informations, consultez On-Demand Capacity Reservations .	25 octobre 2018

Fonctionnalité	Version de l'API	Description	Date de publication
Fourniture de vos propres adresses IP (BYOIP)	2016-11-15	Vous pouvez transférer une partie ou la totalité de votre plage d'adresses IPv4 publiques de votre réseau local vers votre AWS compte. Une fois que vous avez transféré la plage d'adresses AWS, elle apparaît dans votre compte sous forme de pool d'adresses. Vous pouvez créer une adresse IP Elastic à partir de votre groupe d'adresses et l'utiliser avec vos ressources AWS . Pour plus d'informations, consultez Fourniture de vos propres adresses IP (BYOIP) dans Amazon EC2 .	23 octobre 2018
Balises de Hôte dédié à la création et prise en charge de la console	2016-11-15	Vous pouvez baliser vos Hôtes dédiés à la création et gérer vos balises Hôte dédié à l'aide de la console Amazon EC2. Pour plus d'informations, consultez Allouer des Hôtes dédiés .	08 octobre 2018
Prise en charge par la console de la mise à l'échelle planifiée pour le parc d'instances Spot	2016-11-15	Augmente ou réduit la capacité actuelle du flotte en fonction de la date et de l'heure. Pour plus d'informations, consultez Mise à l'échelle du parc d'instances Spot en utilisant la mise à l'échelle planifiée .	20 septembre 2018
Stratégies d'allocation pour les Flottes EC2	2016-11-15	Vous pouvez spécifier si l'affectation de capacité à la demande est traitée par prix (prix le plus bas en premier) ou par priorité (priorité la plus élevée en premier). Vous pouvez spécifier le nombre de groupes d'instances Spot auxquels allouer votre capacité Spot cible. Pour plus d'informations, consultez Stratégies d'allocation pour instances Spot .	26 juillet 2018

Fonctionnalité	Version de l'API	Description	Date de publication
Stratégies d'allocation pour les Parcs d'instances Spot	2016-11-15	Vous pouvez spécifier si l'affectation de capacité à la demande est traitée par prix (prix le plus bas en premier) ou par priorité (priorité la plus élevée en premier). Vous pouvez spécifier le nombre de groupes d'instances Spot auxquels allouer votre capacité Spot cible. Pour plus d'informations, consultez Stratégies d'allocation pour instances Spot .	26 juillet 2018
Automatisation du cycle de vie des instantanés	2016-11-15	Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création et la suppression d'instantanés pour vos volumes EBS. Pour plus d'informations, consultez Amazon Data Lifecycle Manager .	12 juillet 2018
Options d'UC liées aux modèles de lancement	2016-11-15	Lorsque vous créez un modèle de lancement à l'aide des outils de ligne de commande, vous pouvez optimiser les options d'UC afin de les adapter à des charges de travail spécifiques ou à vos besoins métier. Pour plus d'informations, consultez Création d'un modèle de lancement .	11 juillet 2018
Balisage des Hôtes dédiés	2016-11-15	Vous pouvez baliser vos Hôtes dédiés. Pour plus d'informations, consultez Balisage des Hôtes dédiés .	3 juillet 2018
Obtenir la dernière sortie de console	2016-11-15	Vous pouvez récupérer la dernière sortie de console pour certains types d'instances à l'aide de la commande AWS CLI get-console-output .	9 mai 2018

Fonctionnalité	Version de l'API	Description	Date de publication
Optimiser les options d'UC	2016-11-15	Lorsque vous lancez une instance, vous pouvez optimiser les options d'UC pour répondre à des besoins métier ou des charges de travail spécifiques. Pour plus d'informations, consultez Optimiser les options d'UC .	8 mai 2018
EC2 Fleet	2016-11-15	Vous pouvez utiliser la flotte d'instances EC2 pour lancer un groupe d'instances entre différents types d'instance EC2 et zones de disponibilité, et entre les modèles d'achat d'instance à la demande, d'instance réservée et d'instance Spot. Pour plus d'informations, consultez EC2 Fleet .	2 mai 2018
instances à la demande dans des Parcs d'instances Spot	2016-11-15	Vous pouvez inclure une demande de capacité à la demande dans votre demande de parc d'instances Spot pour garantir que vous avez toujours la capacité d'instance. Pour plus d'informations, consultez Parc d'instances Spot .	2 mai 2018
Baliser les instantanés EBS à la création	2016-11-15	Vous pouvez appliquer des balises aux instantanés au moment de la création.	2 avril 2018
Modifier les groupes de placement	2016-11-15	Vous pouvez déplacer une instance à l'intérieur ou à l'extérieur d'un groupe de placement, ou modifier son groupe de placement. Pour plus d'informations, consultez Modifier le groupe de placement d'une instance .	1 mars 2018
ID de ressource plus longs	2016-11-15	Vous pouvez activer le format d'ID long pour d'autres types de ressource. Pour plus d'informations, consultez ID de ressource .	9 février 2018

Fonctionnalité	Version de l'API	Description	Date de publication
Améliorations des performances réseau	2016-11-15	Les instances qui se trouvent en dehors d'un groupe de placement de cluster peuvent à présent profiter d'une bande passante plus élevée pour l'envoi ou la réception de trafic réseau entre d'autres instances ou Amazon S3.	24 janvier 2018
Balisateur de vos adresses IP Elastic	2016-11-15	Vous pouvez baliser vos adresses IP Elastic. Pour plus d'informations, consultez Baliser une adresse IP Elastic .	21 décembre 2017
Amazon Time Sync Service	2016-11-15	Amazon Time Sync Service permet de garder une heure précise sur votre instance. Pour plus d'informations, consultez Définissez l'heure pour votre instance Amazon EC2 .	29 novembre 2017
T2 illimité	2016-11-15	Les instances T2 illimité peuvent dépasser le niveau de base aussi longtemps que nécessaire. Pour plus d'informations, consultez Instance de performance à capacité extensible .	29 novembre 2017
Modèles de lancement	2016-11-15	Un modèle de lancement peut contenir tout ou partie des paramètres permettant de lancer une instance. Il est donc inutile de les spécifier à chaque lancement d'une instance. Pour plus d'informations, consultez Lancer une instance à partir d'un modèle de lancement .	29 novembre 2017
Placement par répartition	2016-11-15	Les groupes de placement par répartition sont recommandés pour les applications ayant un petit nombre d'instances critiques, qui doivent être séparées les unes des autres. Pour plus d'informations, consultez Groupes de placement par répartition .	29 novembre 2017

Fonctionnalité	Version de l'API	Description	Date de publication
Mise en veille prolongée d'instances Spot	2016-11-15	Le service d'instances Spot peut mettre les instances Spot en veille prolongée en cas d'interruption. Pour plus d'informations, consultez Mettre les instances Spot interrompues en veille prolongée .	28 novembre 2017
Suivi de cible du parc d'instances Spot	2016-11-15	Vous pouvez configurer des politiques de suivi des objectifs et d'échelonnement pour votre parc d'instances Spot. Pour plus d'informations, consultez Mise à l'échelle d'un parc d'instances Spot en utilisant une politique de suivi de cible .	17 novembre 2017
Le parc d'instances Spot s'intègre avec Elastic Load Balancing	2016-11-15	Vous pouvez attacher un ou plusieurs équilibres de charge à un parc d'instances Spot.	10 novembre 2017
Fusionner et diviser des instances réservées convertibles	2016-11-15	Vous pouvez échanger (ou fusionner) deux instances réservées convertibles ou plus pour obtenir une nouvelle Instance réservée convertible. Vous pouvez également utiliser le processus de modification pour diviser une Instance réservée convertible en plus petites réservations. Pour plus d'informations, consultez Échanger des instances réservées convertibles .	6 novembre 2017
Modification de la location de VPC	2016-11-15	Vous pouvez modifier l'attribut de location d'instance d'un VPC en remplaçant <code>dedicated</code> par <code>default</code> . Pour plus d'informations, consultez Modifier la location d'un VPC .	16 octobre 2017

Fonctionnalité	Version de l'API	Description	Date de publication
Facturation par seconde	2016-11-15	Amazon EC2 facture l'utilisation Linux par seconde, avec des frais minimum d'une minute.	2 octobre 2017
Arrêt sur une interruption	2016-11-15	Vous pouvez préciser si Amazon EC2 doit arrêter ou résilier les instances Spot lorsqu'elles sont interrompues. Pour plus d'informations, consultez Comportement des interruptions des instances Spot .	18 septembre 2017
Baliser des passerelles NAT	2016-11-15	Vous pouvez baliser votre passerelle NAT. Pour plus d'informations, consultez Etiqueter vos ressources .	7 septembre 2017
Descriptions des règles des groupes de sécurité	2016-11-15	Vous pouvez ajouter des descriptions aux règles des groupes de sécurité. Pour plus d'informations, consultez Règles des groupes de sécurité .	31 août 2017
Elastic Graphics	2016-11-15	Attachez des accélérateurs Elastic Graphics à vos instances pour accélérer les performances graphiques de vos applications.	29 août 2017
Récupération d'adresses IP Elastic	2016-11-15	Si vous avez libéré une adresse IP Elastic à utiliser dans un VPC, vous pouvez essayer de la récupérer. Pour plus d'informations, consultez Récupérer une adresse IP Elastic .	11 août 2017
Identifier les instances du parc d'instances Spot	2016-11-15	Vous pouvez configurer votre parc d'instances Spot pour identifier automatiquement les instances qu'il lance.	24 juillet 2017

Fonctionnalité	Version de l'API	Description	Date de publication
Baliser des ressources pendant la création	2016-11-15	Vous pouvez appliquer des balises à des instances et des volumes au moment de la création. Pour plus d'informations, consultez Etiqueter vos ressources . De plus, vous pouvez utiliser des autorisations de niveau ressources basées sur des balises pour contrôler les balises appliquées. Pour plus d'informations, consultez Accorder l'autorisation de baliser les ressources lors de la création .	28 mars 2017
Effectuez des modifications sur les volumes EBS attachés	2016-11-15	Avec la plupart des volumes EBS attachés à la plupart des instances EC2, vous pouvez modifier la taille de volume, le type et les IOPS sans détacher le volume, ni arrêter l'instance.	13 février 2017
Attachement d'un rôle IAM	2016-11-15	Vous pouvez attacher, détacher ou remplacer un rôle IAM pour une instance existante. Pour plus d'informations, consultez Rôles IAM pour Amazon EC2 .	9 février 2017
instances Spot dédiées	2016-11-15	Vous pouvez exécuter les instances Spot sur un matériel à client unique dans un Virtual Private Cloud (VPC). Pour plus d'informations, consultez Spécifier une location pour votre instances Spot .	19 janvier 2017
Prise en charge d'IPv6	2016-11-15	Vous pouvez associer un bloc d'adresse CIDR IPv6 au VPC et aux sous-réseaux, et attribuer des adresses IPv6 aux instances de votre VPC. Pour plus d'informations, consultez Adressage IP des instances Amazon EC2 .	1er décembre 2016

Fonctionnalité	Version de l'API	Description	Date de publication
Scalabilité automatique du parc d'instances Spot		Vous pouvez désormais configurer des politiques de mise à l'échelle pour votre parc d'instances Spot . Pour plus d'informations, consultez Scalabilité automatique du parc d'instances Spot .	1 septembre 2016
Elastic Network Adapter (ENA)	01-04-2016	Vous pouvez désormais utiliser ENA pour une mise en réseau améliorée. Pour plus d'informations, consultez Prise en charge de la mise en réseau améliorée .	28 juin 2016
Prise en charge améliorée de l'affichage et de la modification des ID longs	01-04-2016	Vous pouvez maintenant afficher et modifier les paramètres d'ID long des autres utilisateurs IAM, des rôles IAM ou de l'utilisateur racine. Pour plus d'informations, consultez ID de ressource .	23 juin 2016
Copiez des instantanés Amazon EBS chiffrés entre les comptes AWS	01-04-2016	Vous pouvez désormais copier des instantanés EBS chiffrés entre AWS comptes.	21 juin 2016
Création d'une capture d'écran d'une console d'instance	01-10-2015	Vous pouvez désormais obtenir des informations supplémentaires lors du débogage d'instances inaccessibles. Pour plus d'informations, consultez Création d'une capture d'écran d'une instance inaccessible .	24 mai 2016
Deux nouveaux types de volumes EBS	01-10-2015	Vous pouvez désormais créer des volumes HDD à débit optimisé (st1) et des volumes HDD à froid (sc1).	19 avril 2016

Fonctionnalité	Version de l'API	Description	Date de publication
Ajout de nouvelles NetworkPacketsOut statistiques NetworkPacketsIn et de nouvelles mesures pour Amazon EC2		Ajout de nouvelles NetworkPacketsOut métriques NetworkPacketsIn et de nouvelles mesures pour Amazon EC2. Pour plus d'informations, consultez Métriques des instances .	23 mars 2016
CloudWatch métriques pour Spot Fleet		Vous pouvez désormais obtenir CloudWatch des statistiques pour votre parc de spots. Pour plus d'informations, consultez CloudWatch métriques pour Spot Fleet .	21 mars 2016
instances planifiées	01-10-2015	Les instances réservées planifiées (instances planifiées) vous permettent d'acheter des réservations de capacité récurrentes sur une base quotidienne, hebdomadaire ou mensuelle, avec une date de début et une durée spécifiées.	13 janvier 2016
ID de ressource plus longs	01-10-2015	Nous introduisons progressivement des ID plus longs pour certains types de ressource Amazon EC2 et Amazon EBS. Durant la période d'abonnement, vous pouvez activer le format d'ID plus long pour les types de ressources pris en charge. Pour plus d'informations, consultez ID de ressource .	13 janvier 2016
ClassicLink Prise en charge du DNS	01-10-2015	Vous pouvez activer le support ClassicLink DNS pour votre VPC afin que les noms d'hôtes DNS adressés entre les instances EC2-Classic liées et les instances du VPC soient convertis en adresses IP privées et non en adresses IP publiques.	11 janvier 2016

Fonctionnalité	Version de l'API	Description	Date de publication
Hôtes dédiés	01-10-2015	Un hôte dédié Amazon EC2 est un serveur physique avec une capacité d'instance dédiée à votre utilisation. Pour plus d'informations, consultez Hôtes dédiés .	23 novembre 2015
Durée d'instance Spot	01-10-2015	Vous pouvez désormais spécifier une durée pour vos instances Spot. Les blocs d'instances Spot ne sont pas pris en charge (janvier 2023).	6 octobre 2015
Demande de modification de parc d'instances Spot	01-10-2015	Vous pouvez désormais modifier la capacité cible de votre demande de parc d'instances Spot. Pour plus d'informations, consultez Modifier une demande de parc d'instances Spot .	29 septembre 2015
Stratégie d'allocation diversifiée de parc d'instances Spot	15-04-2015	Vous pouvez désormais allouer des instances Spot dans plusieurs groupes d'instances Spot à l'aide d'une seule demande de parc d'instances Spot. Pour plus d'informations, consultez Stratégies d'allocation pour instances Spot .	15 septembre 2015
Pondération d'instance de parc d'instances Spot	15-04-2015	Vous pouvez désormais définir les unités de capacité par lesquelles chaque type d'instance contribue aux performances de votre application et ajuster en conséquence le montant que vous êtes prêt à payer pour des instances Spot pour chaque pool d'instances Spot. Pour plus d'informations, consultez Pondération d'instance de parc d'instances Spot .	31 août 2015

Fonctionnalité	Version de l'API	Description	Date de publication
Nouvelle action d'alarme de redémarrage et nouveau rôle IAM à utiliser avec les actions d'alarme		Ajout de la nouvelle action d'alarme de redémarrage et du nouveau rôle IAM à utiliser avec les actions d'alarme. Pour plus d'informations, consultez Créer des alarmes qui arrêtent, finissent, redémarrent ou récupèrent une instance.	23 juillet 2015
Spot Fleets	15-04-2015	Vous pouvez gérer un ensemble, ou une flotte d'instances Spot au lieu de gérer des demandes d'instance Spot distinctes. Pour plus d'informations, consultez Parc d'instances Spot.	18 mai 2015
Migrer les adresses IP Elastic vers EC2-Classic	15-04-2015	Vous pouvez migrer une adresse IP Elastic que vous avez allouée pour être utilisée dans EC2-Classic afin qu'elle soit utilisée dans un VPC.	15 mai 2015
Importation de machines virtuelles avec plusieurs disques comme AMI	01-03-2015	Le processus VM Import prend désormais en charge l'importation de machines virtuelles avec plusieurs disques comme AMI. Pour plus d'informations, consultez Importation d'un ordinateur virtuel comme image à l'aide de VM Import/Export dans le VM Import/Export Guide de l'utilisateur.	23 avril 2015
Systems Manager		Systems Manager vous permet de configurer et de gérer vos instances EC2.	17 février 2015
Systems Manager pour Microsoft SCVMM 1.5		Vous pouvez désormais utiliser Systems Manager pour Microsoft SCVMM pour lancer une instance et importer une machine virtuelle depuis SCVMM vers Amazon EC2.	21 janvier 2015

Fonctionnalité	Version de l'API	Description	Date de publication
Récupération automatique des instances EC2		<p>Vous pouvez créer une CloudWatch alarme Amazon qui surveille une instance Amazon EC2 et la récupère automatiquement si elle est endommagée en raison d'une défaillance matérielle sous-jacente ou d'un problème nécessitant une AWS intervention pour être réparée. Une instance récupérée est identique à l'instance d'origine, y compris son ID d'instance, les adresses IP privées et toutes les métadonnées d'instance.</p> <p>Pour plus d'informations, consultez Résilience de l'instance.</p>	12 janvier 2015
ClassicLink	01-10-2014	ClassicLink vous permet de lier votre instance EC2-Classic à un VPC de votre compte. Vous pouvez associer des groupes de sécurité VPC à l'instance EC2-Classic en activant la communication entre votre instance EC2-Classic et des instances de votre VPC à l'aide d'adresses IP privées.	7 janvier 2015
Avis de résiliation d'instance Spot		<p>Le meilleur moyen de vous protéger contre une interruption d'instance Spot est de faire en sorte que votre application soit tolérante aux pannes au niveau de son architecture. En outre, vous pouvez tirer parti des avis de résiliation d'instance Spot, qui vous préviennent deux minutes avant qu'Amazon EC2 n'interrompte ou ne résilie votre instance Spot.</p> <p>Pour plus d'informations, consultez Avis d'interruption d'instance Spot.</p>	5 janvier 2015

Fonctionnalité	Version de l'API	Description	Date de publication
Systems Manager pour Microsoft SCVMM		Systems Manager for Microsoft SCVMM fournit une easy-to-use interface simple pour gérer les AWS ressources, telles que les instances EC2, à partir de Microsoft SCVMM.	29 octobre 2014
Prise en charge de la pagination DescribeVolumes	01-09-2014	L'appel de l'API DescribeVolumes prend désormais en charge la pagination des résultats à l'aide des paramètres MaxResults et NextToken . Pour plus d'informations, consultez DescribeVolumes le manuel Amazon EC2 API Reference.	23 octobre 2014
Ajout de la prise en charge d'Amazon CloudWatch Logs		Vous pouvez utiliser Amazon CloudWatch Logs pour surveiller, stocker et accéder à votre système, à votre application et aux fichiers journaux personnalisés à partir de vos instances ou d'autres sources. Vous pouvez ensuite récupérer les données de journal associées depuis CloudWatch Logs à l'aide de la CloudWatch console Amazon, CloudWatch Logs des commandes Logs de la AWS CLI ou du SDK CloudWatch Logs.	10 juillet 2014
Nouvelle page Service Limits EC2		Utilisez la page Service Limits EC2 de la console Amazon EC2 afin d'afficher les limites actuelles des ressources fournies par Amazon EC2 et Amazon VPC, région par région.	19 juin 2014

Fonctionnalité	Version de l'API	Description	Date de publication
Volumes Amazon EBS SSD à usage général	01-05-2014	Les volumes SSD à usage général offrent un stockage économique idéal pour un large éventail de charges de travail. Ces volumes offrent des latences inférieures à 10 millisecondes, la capacité d'augmenter jusqu'à 3 000 IOPS pour une durée étendue et une performance de base de 3 IOPS/Gio. La taille des volumes polyvalents peut aller de 1 Gio à 1 Tio.	16 juin 2014
AWS Pack de gestion		AWS Le pack d'administration est désormais compatible avec System Center Operations Manager 2012 R2.	22 mai 2014
Amazon EBS encryption	01-05-2014	Chiffrement Amazon EBS offre un chiffrement transparent des instantanés et des volumes de données EBS sans que vous ayez à développer et à maintenir une infrastructure de gestion de clés sécurisée. Le chiffrement EBS assure la sécurité des données au repos en chiffrant vos données à l'aide de clés Clés gérées par AWS. Le chiffrement est effectué sur les serveurs hébergeant des instances EC2, assurant le chiffrement des données lorsqu'elles se déplacent entre les instances EC2 et le stockage EBS.	21 mai 2014
Amazon EC2 Usage Reports		Amazon EC2 Usage Reports est un ensemble de rapports qui affiche les données de coût et d'utilisation d'EC2.	28 janvier 2014

Fonctionnalité	Version de l'API	Description	Date de publication
Importation de machines virtuelles Linux	15-10-2013	Le processus VM Import prend désormais en charge l'importation d'instances Linux. Pour plus d'informations, consultez le VM Import/Export Guide de l'utilisateur .	16 décembre 2013
Autorisations au niveau des ressources pour RunInstances	15-10-2013	Vous pouvez désormais créer des politiques AWS Identity and Access Management pour contrôler les autorisations au niveau des ressources pour l'action d'API Amazon RunInstances EC2. Pour plus d'informations et obtenir des exemples de stratégie, consultez Identity and Access Management pour Amazon EC2 .	20 novembre 2013
Lancement d'une instance depuis AWS Marketplace		Vous pouvez désormais lancer une instance à l'AWS Marketplace aide de l'assistant de lancement Amazon EC2. Pour plus d'informations, consultez Lancer une AWS Marketplace instance .	11 novembre 2013
Nouvel Assistant de lancement		L'Assistant de lancement EC2 a été refondu. Pour plus d'informations, consultez Lancer une instance à l'aide de l'ancien assistant de lancement d'instance .	10 octobre 2013
Modification des types d'instances réservées	01-10-2013	Vous pouvez désormais modifier le type d'instances des instances réservées Linux d'une même famille (par exemple, M1, M2, M3, C1). Pour plus d'informations, consultez Modifier instances réservées .	09 octobre 2013
Modification des instances réservées Amazon EC2	15-08-2013	Vous pouvez désormais modifier les instances réservées d'une région. Pour plus d'informations, consultez Modifier instances réservées .	11 septembre 2013

Fonctionnalité	Version de l'API	Description	Date de publication
Attribution d'une adresse IP publique	15-07-2013	Vous pouvez désormais attribuer une adresse IP publique quand vous lancez une instance dans VPC. Pour plus d'informations, consultez Attribuer une adresse IPv4 publique lors du lancement d'une instance .	20 août 2013
Attribution d'autorisations au niveau des ressources	15-06-2013	Amazon EC2 prend en charge les nouveaux Amazon Resource Names (ARN) et clés de condition. Pour plus d'informations, consultez Stratégies IAM pour Amazon EC2 .	8 juillet 2013
Copies d'instantané incrémentielles	01-02-2013	Vous pouvez désormais effectuer des copies d'instantané incrémentielles.	11 juin 2013
AWS Pack de gestion		Le pack d' AWS administration relie les instances Amazon EC2 aux systèmes d'exploitation Windows ou Linux qui y sont exécutés. Le pack d' AWS administration est une extension de Microsoft System Center Operations Manager.	8 mai 2013
Nouvelle page Balises		Nouvelle page Balises dans la console Amazon EC2. Pour plus d'informations, consultez Baliser vos ressources Amazon EC2 .	04 avril 2013
Copier une AMI d'une région vers une autre	01-02-2013	Vous pouvez copier une AMI d'une région à l'autre, ce qui vous permet de lancer des instances cohérentes dans plusieurs AWS régions rapidement et facilement. Pour plus d'informations, consultez Copier une AMI .	11 mars 2013

Fonctionnalité	Version de l'API	Description	Date de publication
Lancer une instance dans un VPC par défaut	01-02-2013	Votre AWS compte est capable de lancer des instances dans EC2-Classique ou dans un VPC, ou uniquement dans un VPC, sur une base. region-by-region Si vous pouvez uniquement lancer des instances dans un VPC, nous créerons un VPC par défaut pour vous. Lorsque vous lancez une instance, nous la lançons dans votre VPC par défaut, sauf si vous créez un VPC personnalisé et que vous le spécifiez au lancement de l'instance.	11 mars 2013
Copie d'instantané EBS	01-12-2012	Vous pouvez utiliser les copies d'instantané pour créer des sauvegardes de données, des volumes Amazon EBS ou des Amazon Machine Images (AMI).	17 décembre 2012
Métriques EBS mises à jour et contrôles de statut pour les volumes Provisioned IOPS SSD	01-10-2012	Métriques EBS mises à jour pour inclure deux nouvelles métriques pour les volumes Provisioned IOPS SSD. Ajout de nouveaux contrôles de statut pour les volumes Provisioned IOPS SSD.	20 novembre 2012
État de demande d'instance Spot	01-10-2012	L'état de demande d'instance Spot simplifie la détermination de l'état de vos demandes Spot.	14 octobre 2012

Fonctionnalité	Version de l'API	Description	Date de publication
Marketplace des instances réservées Amazon EC2	15-08-2012	Le Marketplace d'instance réservée met en correspondance les vendeurs ayant des instances réservées Amazon EC2 dont ils n'ont plus besoin et les acheteurs en quête d'achat de capacité supplémentaire. Les instances réservées achetées et vendues via le Marketplace d'instance réservée fonctionnent comme toute autre instance réservée, si ce n'est qu'il peut ne leur rester qu'une durée standard complète et qu'elles peuvent être vendues à différents prix.	11 septembre 2012
Provisioned IOPS SSD pour Amazon EBS	20-07-2012	Les volumes Provisioned IOPS SSD offrent des performances élevées et prévisibles pour les charges de travail gourmandes en I/O, telles que les applications de base de données, qui reposent sur des temps de réponse rapides et réguliers.	31 juillet 2012
Rôles IAM sur les instances Amazon EC2	01-06-2012	Les rôles IAM pour Amazon EC2 fournissent : <ul style="list-style-type: none"> • AWS clés d'accès pour les applications exécutées sur des instances Amazon EC2. • Rotation automatique des clés AWS d'accès sur l'instance Amazon EC2. • Autorisations granulaires pour les applications exécutées sur des instances Amazon EC2 qui adressent des demandes à AWS vos services. 	11 juin 2012

Fonctionnalité	Version de l'API	Description	Date de publication
Fonctions d'instance Spot qui facilitent le démarrage et la gestion d'une interruption potentielle.		<p>Vous pouvez désormais gérer vos instances Spot comme suit :</p> <ul style="list-style-type: none"> • Spécifiez le montant que vous êtes prêt à payer pour des instances Spot à l'aide de configurations de lancement Auto Scaling et configurez un calendrier pour indiquer ce montant pour des instances Spot. Pour plus d'informations, consultez Lancement d'Instances Spot dans votre groupe Auto Scaling dans le Amazon EC2 Auto Scaling Guide de l'utilisateur. • Obtenez des notifications quand les instances sont lancées ou terminées. • Utilisez AWS CloudFormation des modèles pour lancer des instances Spot dans une pile contenant AWS des ressources. 	7 juin 2012
Exportation d'instance EC2 et horodatage des contrôles de statut pour Amazon EC2	01-05-2012	<p>Ajout de la prise en charge de l'exportation des instances Windows Server que vous avez importées à l'origine dans EC2.</p> <p>Ajout de la prise en charge des horodatages sur le statut d'instance et le statut système pour indiquer la date et l'heure auxquelles un contrôle d'état a échoué.</p>	25 mai 2012

Fonctionnalité	Version de l'API	Description	Date de publication
Exportation d'instance EC2 et horodatages des contrôles de statut d'instance et de statut système pour Amazon VPC	01-05-2012	<p>Ajout de la prise en charge de l'exportation d'instance EC2 vers Citrix Xen, Microsoft Hyper-V et VMware vSphere.</p> <p>Ajout de la prise en charge des horodatages dans les contrôles de statut d'instance et de statut système.</p>	25 mai 2012
AWS Marketplace AMI	01-04-2012	Ajout du support pour les AWS Marketplace AMI.	19 avril 2012
Niveaux de tarification des instances réservées	15-12-2011	Ajout d'une nouvelle section expliquant comment tirer parti de la tarification des remises intégrée aux niveaux de tarification des instances réservées.	5 mars 2012
Interfaces ENI (interface réseau Elastic) pour les instances EC2 dans Amazon Virtual Private Cloud	01-12-2011	Ajout d'une nouvelle section sur les interfaces ENI (interface réseau Elastic) pour les instances EC2 d'un VPC. Pour plus d'informations, consultez Interfaces réseau Elastic .	21 décembre 2011
Nouveaux types d'offre pour les instances réservées Amazon EC2	01-11-2011	Vous avez le choix entre différentes offres d'instances réservées qui prennent en compte votre utilisation projetée de l'instance.	01 décembre 2011

Fonctionnalité	Version de l'API	Description	Date de publication
Statut d'instance Amazon EC2	01-11-2011	Vous pouvez consulter des informations supplémentaires sur le statut de vos instances , y compris les événements planifiés par et AWS susceptibles d'avoir un impact sur vos instances. Ces activités opérationnelles incluent les redémarrages d'instance requis pour appliquer les mises à jour logicielles ou les correctifs de sécurité, ou les exigences d'instance requises en cas de problèmes matériels. Pour plus d'informations, consultez Surveiller le statut de vos instances .	16 novembre 2011
instances Spot dans Amazon VPC	15-07-2011	Ajout d'informations sur la prise en charge des instances Spot dans Amazon VPC. Avec cette mise à jour, les utilisateurs peuvent lancer des instances Spot dans un Virtual Private Cloud (VPC). En lançant des instances Spot dans un VPC, les utilisateurs d'instances Spot peuvent profiter des avantages de Amazon VPC.	11 octobre 2011
Processus VM Import simplifié pour les utilisateurs des outils de la CLI	15-07-2011	Le processus VM Import est simplifié avec la fonctionnalité améliorée d'ImportInstance et d'ImportVolume , qui désormais effectuent le chargement des images dans Amazon EC2 après avoir créé la tâche d'importation. De plus, avec l'introduction de la commande ResumeImport , les utilisateurs peuvent redémarrer un chargement incomplet au point où la tâche s'est arrêtée.	15 septembre 2011

Fonctionnalité	Version de l'API	Description	Date de publication
Prise en charge de l'importation au format de fichier VHD		VM Import peut désormais importer les fichiers image de machine virtuelle au format VHD. Le format de fichier VHD compatible avec les plateformes de virtualisation Citrix Xen et Microsoft Hyper-V. Avec cette version, VM Import prend désormais en charge les formats d'image RAW, VHD et VMDK (compatible VMware ESX). Pour plus d'informations, consultez le VM Import/Export Guide de l'utilisateur .	24 août 2011
Mise à jour d'Amazon EC2 VM Import Connector pour VMware vCenter		Ajout d'informations sur la version 1.1 version de l'appliance virtuelle Amazon EC2 VM Import Connector pour VMware vCenter (connecteur). Cette mise à jour inclut la prise en charge du proxy pour l'accès Internet, une meilleure gestion des erreurs, une précision accrue de la barre d'avancement des tâches et plusieurs correctifs de bogue.	27 juin 2011
Modifications de tarification des zones de disponibilité des instances Spot	15-05-2011	Ajout d'informations sur la fonction de tarification des zones de disponibilité des instances Spot. Dans cette version, nous avons ajouté les options de tarification des zones de disponibilité, comme parties intégrantes des informations retournées quand vous interrogez les demandes d'instance Spot et l'historique des prix Spot. Ces ajouts permettent de déterminer plus facilement le prix requis pour lancer une instance Spot dans une zone de disponibilité particulière.	26 mai 2011

Fonctionnalité	Version de l'API	Description	Date de publication
AWS Identity and Access Management		Ajout d'informations sur AWS Identity and Access Management (IAM), qui permettent aux utilisateurs de spécifier les actions Amazon EC2 qu'ils peuvent utiliser avec les ressources Amazon EC2 en général. Pour plus d'informations, consultez Identity and Access Management pour Amazon EC2 .	26 avril 2011
instances dédiées		Lancées au sein de votre Amazon Virtual Private Cloud (Amazon VPC), les instances dédiées sont des instances physiquement isolées au niveau matériel hôte. Les instances dédiées vous permettent de tirer parti d'Amazon VPC et du AWS cloud, avec des avantages tels que le provisionnement élastique à la demande et le paiement uniquement pour ce que vous utilisez, tout en isolant vos instances de calcul Amazon EC2 au niveau matériel. Pour plus d'informations, consultez Dedicated instances .	27 mars 2011
Mises à jour de la console de AWS gestion relatives aux instances réservées		Les mises à jour AWS de la console de gestion permettent aux utilisateurs de consulter plus facilement leurs instances réservées et d'acheter des instances réservées supplémentaires, y compris des instances réservées dédiées.	27 mars 2011
Informations de métadonnées	2011-01-01	Ajout d'informations sur les métadonnées pour refléter les modifications de la version 2011-01-01. Pour plus d'informations, consultez Utiliser des métadonnées d'instance et Catégories de métadonnées d'instance .	11 mars 2011

Fonctionnalité	Version de l'API	Description	Date de publication
Amazon EC2 VM Import Connector pour VMware vCenter		Ajout d'informations sur l'appliance virtuelle Amazon EC2 VM Import Connector pour VMware vCenter (connecteur). Le connecteur est un plugin pour VMware vCenter qui s'intègre à VMware vSphere Client et fournit une interface utilisateur graphique que vous pouvez utiliser pour importer vos machines virtuelles VMware sur Amazon EC2.	3 mars 2011
Forcer le détachement du volume		Vous pouvez désormais utiliser le AWS Management Console pour forcer le détachement d'un volume Amazon EBS d'une instance.	23 février 2011
Protection de la fin d'instance		Vous pouvez désormais utiliser la console AWS de gestion pour empêcher la résiliation d'une instance. Pour plus d'informations, consultez Activer la protection de la résiliation .	23 février 2011
VM Import	15-11-2010	Ajout d'informations sur VM Import, qui vous permet d'importer un volume ou une machine virtuelle dans Amazon EC2. Pour plus d'informations, consultez le VM Import/Export Guide de l'utilisateur .	15 décembre 2010
Surveillance basique pour les instances	31-08-2010	Ajout d'informations sur la surveillance basique pour les instances EC2.	12 décembre 2010
Filtres et balises	31-08-2010	Ajout d'informations sur les ressources d'affichage, de filtrage et de balisage. Pour plus d'informations, consultez Lister et filtrer vos ressources et Baliser vos ressources Amazon EC2 .	19 septembre 2010

Fonctionnalité	Version de l'API	Description	Date de publication
Lancement d'instance idempotente	31-08-2010	Ajout d'informations pour garantir l'idempotence lors de l'exécution des instances.	19 septembre 2010
AWS Identity and Access Management pour Amazon EC2		Amazon EC2 s'intègre désormais avec AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Identity and Access Management pour Amazon EC2 .	2 septembre 2010
Désignation de l'adresse IP Amazon VPC	15-06-2010	Les utilisateurs Amazon VPC peuvent désormais spécifier l'adresse IP pour attribuer une instance lancée dans un VPC.	12 juillet 2010
CloudWatch Surveillance Amazon pour Amazon EBS Volumes		La CloudWatch surveillance Amazon est désormais automatiquement disponible pour les volumes Amazon EBS.	14 juin 2010
instances réservées avec Windows		Amazon EC2 prend désormais en charge les instances réservées avec Windows.	22 février 2010

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.